(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－164885
（P2002－164885A）
(43)公開日　平成14年６月７日(2002.6.7)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
H04L 9/32		G06F 13/00	540S	5J104
G06F 13/00	540	G09C 1/00	640Z	
G09C 1/00	640		660A	
	660		660D	
		G10K 15/02		

審査請求　未請求　請求項の数15　ＯＬ　（全 37 頁）　最終頁に続く

(21)出願番号　特願2000－362914(P2000－362914)

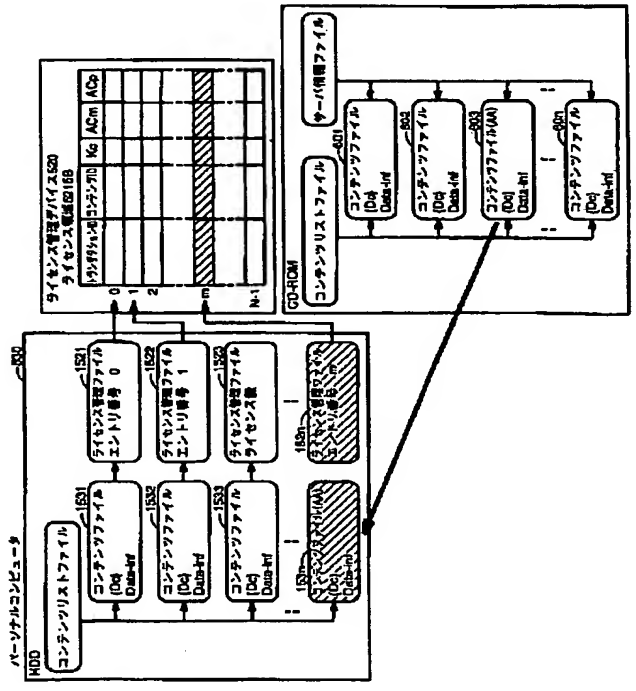
(22)出願日　平成12年11月29日(2000.11.29)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(71)出願人　000136136
株式会社ピーエフユー
石川県河北郡宇ノ気町字宇野気ヌ98番地の２
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　データ端末装置

(57)【要約】
【課題】　記録媒体から暗号化コンテンツデータを取得すると暗号化コンテンツデータを再生するライセンスを取得するデータ端末装置を提供する。
【解決手段】　パーソナルコンピュータは、ＣＤ－ＲＯＭから暗号化コンテンツデータ、コンテンツファイル６０１～６０ｎ、およびサーバ情報ファイルをハードディスク５３０にコピーし、サーバ情報ファイルに含まれるアクセス手段およびアクセス先のアドレスに基づいて配信サーバへ暗号化コンテンツデータのライセンスの配信を要求し、ライセンスを受信する。そして、受信したライセンスを内蔵するライセンス管理デバイス５２０のメモリのライセンス領域５２１５Ｂに格納する。



【特許請求の範囲】

【請求項１】　暗号化コンテンツデータと前記暗号化コンテンツデータを再生するためのライセンスの取得に必要なサーバ情報ファイルとを含む記録媒体から前記暗号化コンテンツデータを取得し、前記サーバ情報ファイルに基づいて前記ライセンスを配信サーバから取得するデータ端末装置であって、
前記暗号化コンテンツデータおよび前記サーバ情報ファイルを前記記録媒体から取得する媒体駆動部と、
前記媒体駆動部によって取得されたサーバ情報ファイルの内容に応じて前記配信サーバとの接続手段を決定し、その決定した接続手段によって前記配信サーバに接続して前記ライセンスの配信を要求し、前記配信サーバから前記ライセンスを受信する制御部と、
前記媒体駆動部によって取得された暗号化コンテンツデータを記憶する記憶部と、
前記配信サーバから受信したライセンスを格納するデバイス部とを備えるデータ端末装置。

【請求項２】　前記制御部は、前記媒体駆動部が前記記録媒体から前記サーバ情報ファイルを取得できないとき、ユーザの指示によって前記配信サーバに接続する、請求項１に記載のデータ端末装置。

【請求項３】　前記制御部は、前記決定された接続手段に適したアドレスを前記サーバ情報ファイルから取得し、その取得したアドレスに基づいて前記配信サーバに接続する、請求項１に記載のデータ端末装置。

【請求項４】　前記制御部は、前記デバイス部が保持する認証データを前記配信サーバへ送信し、前記配信サーバにおいて前記認証データが認証されると前記配信サーバから前記ライセンスを受信する、請求項１から請求項３のいずれか１項に記載のデータ端末装置。

【請求項５】　前記制御部は、前記デバイス部が保持する公開暗号鍵を前記配信サーバへ送信し、前記配信サーバから前記公開暗号鍵によって暗号化されたライセンスを受信する、請求項４に記載のデータ端末装置。

【請求項６】　前記記憶部は、前記媒体駆動部によって前記記録媒体から取得され、かつ、前記暗号化コンテンツデータと、前記暗号化コンテンツデータに関する平文情報とを格納するコンテンツファイルと、
前記コンテンツファイルに対応して設けられ、前記デバイス部における前記ライセンスの格納領域を指定するための登録番号を格納するライセンス管理ファイルとをさらに記憶する、請求項１から請求項３のいずれか１項に記載のデータ端末装置。

【請求項７】　前記暗号化コンテンツデータを前記記憶部から取得し、前記取得した暗号化コンテンツデータのライセンスを前記デバイス部から取得し、その取得したライセンスによって前記暗号化コンテンツデータを再生する再生部をさらに備える、請求項１から請求項６のいずれか１項に記載のデータ端末装置。

【請求項８】　前記再生部は、前記デバイス部に対する認証データを保持し、前記認証データが前記デバイス部において認証されると、前記デバイス部から前記ライセンスを取得する、請求項７に記載のデータ端末装置。

【請求項９】　記録媒体から暗号化コンテンツデータと前記暗号化コンテンツデータを再生するためのライセンスの取得に必要なサーバ情報ファイルとを読取り可能なデータ端末装置から前記暗号化コンテンツデータおよび前記サーバ情報ファイルを取得し、前記サーバ情報ファイルに基づいて前記ライセンスを配信サーバから取得し、前記取得した暗号化コンテンツデータおよびライセンスをデータ記録装置に記録するデータ端末装置であって、
前記データ記録装置との間でのデータの授受を制御するインタフェースと、
前記配信サーバとの送受信を行なう送受信部と、
前記取得したサーバ情報ファイルの内容に応じて前記配信サーバとの接続手段を決定し、その決定した接続手段によって前記送受信部を介して前記配信サーバに接続して前記ライセンスの配信を要求し、前記配信サーバから前記送受信部を介して前記ライセンスを受信する制御部とを備え、
前記制御部は、前記取得した暗号化コンテンツデータおよびライセンスを前記インタフェースを介して前記データ記録装置へ出力する、データ端末装置。

【請求項１０】　前記制御部は、前記データ端末装置から前記サーバ情報ファイルを取得できないとき、ユーザの指示によって前記配信サーバに接続する、請求項９に記載のデータ端末装置。

【請求項１１】　前記制御部は、前記決定された接続手段に適したアドレスを前記サーバ情報ファイルから取得し、その取得したアドレスに基づいて前記配信サーバに接続する、請求項９に記載のデータ端末装置。

【請求項１２】　前記制御部は、前記データ記録措置が保持する認証データを前記配信サーバへ送信し、前記配信サーバにおいて前記認証データが認証されると前記配信サーバから前記ライセンスを受信する、請求項９から請求項１１のいずれか１項に記載のデータ端末装置。

【請求項１３】　前記制御部は、前記データ記録装置が保持する公開暗号鍵を前記配信サーバへ送信し、前記配信サーバから前記公開暗号鍵によって暗号化されたライセンスを受信する、請求項１２に記載のデータ端末装置。

【請求項１４】　前記暗号化コンテンツデータおよび前記ライセンスを前記データ記録装置から取得し、その取得したライセンスによって前記暗号化コンテンツデータを再生する再生部をさらに備える、請求項９から請求項１３のいずれか１項に記載のデータ端末装置。

【請求項１５】　前記再生部は、前記データ記録装置に対する認証データを保持し、前記認証データが前記デー

タ記録装置において認証されると、前記データ記録装置から前記ライセンスを取得する、請求項１４に記載のデータ端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して著作権料として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽データとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されること、あるいは、複製できても利用されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンス鍵と、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。

【００１５】

【発明が解決しようとする課題】しかし、記録媒体に暗号化音楽データを再生するライセンスも記録して販売すると、不正にライセンスが複製されたり、他の装置へ移動されたりするため、通常、記録媒体には暗号化コンテンツデータだけを記録して販売する。そのため、その記録媒体を購入しただけでは、暗号化コンテンツデータを再生することができない。

【００１６】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、記録媒体から暗号化コンテンツデータを取得すると暗号化コンテンツデータを再生するライセンスを取得するデータ端末装置を提供することである。

【００１７】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、暗号化コンテンツデータと暗号化コンテンツデータを再生するためのライセンスの取得に必要なサーバ情報ファイルとを含む記録媒体から暗号化コンテンツデータを取得し、サーバ情報ファイルに基づいてライセンスを配信サーバから取得するデータ端末装置であって、暗号化コンテンツデータおよびサーバ情報ファイルを記録媒体から取得する媒体駆動部と、媒体駆動部によって取得されたサーバ情報ファイルの内容に応じて配信サーバとの接続手段を決定し、その決定した接続手段によって配信サーバに接続してライセンスの配信を要求し、配信サーバからライセンスを受信する制御部と、媒体駆動部によって取得された暗号化コンテンツデータを記憶する記憶部と、配信サーバから受信したライセンスを格納するデバイス部とを備える。

【００１８】この発明によるデータ端末装置においては、配信サーバへアクセスするのに必要な情報が記録媒体に記録されたサーバ情報ファイルから取得され、その取得された情報によって暗号化コンテンツデータの再生に必要なライセンスが配信サーバから受信され、データ記録装置に記録される。

【００１９】したがって、この発明によれば、記録媒体に記録されたサーバ情報ファイルに基づいて暗号化コンテンツデータを再生するライセンスを取得できる。

【００２０】好ましくは、データ端末装置の制御部は、媒体駆動部が記録媒体からサーバ情報ファイルを取得できないとき、ユーザの指示によって配信サーバに接続する。

【００２１】記録媒体にサーバ情報ファイルが記録されていないときは、ユーザからの指示を待ち、入力されたユーザの指示に従って配信サーバに接続される。

【００２２】したがって、この発明によれば、サーバ情報ファイルを含まない記録媒体から暗号化コンテンツデータを取得した場合でも、配信サーバからライセンスを取得できる。

【００２３】好ましくは、データ端末装置の制御部は、決定された接続手段に適したアドレスをサーバ情報ファイルから取得し、その取得したアドレスに基づいて配信サーバに接続する。

【００２４】データ端末装置においては、制御部は、サーバ情報ファイルの内容に応じて、たとえば、インターネット、電話回線等の接続手段を決定し、ＵＲＬまたは電話番号によって配信サーバに接続する。

【００２５】したがって、この発明によれば、各種の機器に応じてライセンスを自動的に取得できる。

【００２６】好ましくは、データ端末装置の制御部は、デバイス部が保持する認証データを配信サーバへ送信し、配信サーバにおいて認証データが認証されると配信サーバからライセンスを受信する。

【００２７】配信サーバにおいてデータ端末装置が正規の端末装置であると認識されると、データ端末装置は配信サーバからライセンスを受信する。

【００２８】したがって、この発明によれば、不正に暗号化コンテンツデータに対してライセンスを配信することを防止できる。

【００２９】好ましくは、データ端末装置の制御部は、デバイス部が保持する公開暗号鍵を配信サーバへ送信し、配信サーバから公開暗号鍵によって暗号化されたライセンスを受信する。

【００３０】データ端末装置は、公開暗号方式によってライセンスを取得する。したがって、この発明によれば、セキュリティ強度を高くしてライセンスを取得できる。

【００３１】好ましくは、データ端末装置の記憶部は、媒体駆動部によって記録媒体から取得され、かつ、暗号化コンテンツデータと、暗号化コンテンツデータに関する平文情報とを格納するコンテンツファイルと、コンテンツファイルに対応して設けられ、デバイス部におけるライセンスの格納領域を指定するための登録番号を格納するライセンス管理ファイルとをさらに記憶する。

【００３２】暗号化コンテンツデータの名称に対応して登録番号を格納するライセンス管理ファイルが設けられ、その登録番号によってライセンスを格納する領域が指定される。

【００３３】したがって、この発明によれば、登録番号によってライセンスを暗号化コンテンツデータに対応づけることができる。

【００３４】好ましくは、データ端末装置は、暗号化コンテンツデータを記憶部から取得し、その取得した暗号化コンテンツデータのライセンスをデバイス部から取得し、その取得したライセンスによって暗号化コンテンツデータを再生する再生部をさらに備える。

【００３５】ライセンスが取得されたデータ端末装置においては、再生部によって暗号化コンテンツデータが再生される。

【００３６】したがって、この発明によれば、記録媒体から暗号化コンテンツデータを取得し、かつ、暗号化コンテンツデータを再生できる。

【００３７】好ましくは、データ端末装置の再生部は、デバイス部に対する認証データを保持し、認証データがデバイス部において認証されると、デバイス部からライセンスを取得する。

【００３８】ライセンスを保持するデバイス部において、ライセンスの送信を要求する再生部の正当性が確認

されると再生部はライセンスを取得する。

【００３９】したがって、この発明によれば、不正な暗号化コンテンツデータの再生を防止できる。

【００４０】また、この発明によるデータ端末装置は、記録媒体から暗号化コンテンツデータと暗号化コンテンツデータを再生するためのライセンスの取得に必要なサーバ情報ファイルとを読取り可能なデータ端末装置から暗号化コンテンツデータおよびサーバ情報ファイルを取得し、サーバ情報ファイルに基づいてライセンスを配信サーバから取得し、取得した暗号化コンテンツデータおよびライセンスをデータ記録装置に記録するデータ端末装置であって、データ記録装置との間でのデータの授受を制御するインタフェースと、配信サーバとの送受信を行なう送受信部と、取得したサーバ情報ファイルの内容に応じて配信サーバとの接続手段を決定し、その決定した接続手段によって送受信部を介して配信サーバに接続してライセンスの配信を要求し、配信サーバから送受信部を介してライセンスを受信する制御部とを備え、制御部は、取得した暗号化コンテンツデータおよびライセンスをインターフェースを介してデータ記録装置へ出力する。

【００４１】記録媒体の駆動手段を持たないデータ端末装置では、記録媒体の駆動手段を持つデータ端末装置から暗号化コンテンツデータおよびサーバ情報ファイルを送ってもらい、そのサーバ情報ファイルに基づいて暗号化コンテンツデータを再生するライセンスを配信サーバから受信する。

【００４２】したがって、この発明によれば、記録媒体の駆動手段を持たないデータ端末装置のユーザでも、記録媒体に記録されて販売された暗号化コンテンツデータを再生可能である。

【００４３】好ましくは、データ端末装置の制御部は、データ端末装置からサーバ情報ファイルを取得できないとき、ユーザの指示によって配信サーバに接続する。

【００４４】データ端末装置からサーバ情報ファイルが送られてこないときは、ユーザからの指示を待ち、入力されたユーザの指示に従って配信サーバに接続される。

【００４５】したがって、この発明によれば、サーバ情報ファイルを含まない記録媒体から暗号化コンテンツデータを取得した場合でも、配信サーバからライセンスを取得できる。

【００４６】好ましくは、データ端末装置の制御部は、決定された接続手段に適したアドレスをサーバ情報ファイルから取得し、その取得したアドレスに基づいて配信サーバに接続する。

【００４７】データ端末装置においては、制御部は、サーバ情報ファイルの内容に応じて、たとえば、インターネット、電話回線等の接続手段を決定し、ＵＲＬまたは電話番号によって配信サーバに接続する。

【００４８】したがって、この発明によれば、各種の機器に応じてライセンスを自動的に取得できる。

【００４９】好ましくは、データ端末装置の制御部は、データ記録措置が保持する認証データを配信サーバへ送信し、配信サーバにおいて認証データが認証されると配信サーバからライセンスを受信する。

【００５０】配信サーバにおいてデータ端末装置が正規の端末装置であると認識されると、データ端末装置は配信サーバからライセンスを受信する。

【００５１】したがって、この発明によれば、不正に暗号化コンテンツデータに対してライセンスを配信することを防止できる。

【００５２】好ましくは、データ端末装置の制御部は、データ記録装置が保持する公開暗号鍵を配信サーバへ送信し、配信サーバから公開暗号鍵によって暗号化されたライセンスを受信する。

【００５３】データ端末装置は、公開暗号方式によってライセンスを取得する。したがって、この発明によれば、セキュリティ強度を高くしてライセンスを取得できる。

【００５４】好ましくは、データ端末装置は、暗号化コンテンツデータおよびライセンスをデータ記録装置から取得し、その取得したライセンスによって暗号化コンテンツデータを再生する再生部をさらに備える。

【００５５】ライセンスが取得されたデータ端末装置においては、再生部によって暗号化コンテンツデータが再生される。

【００５６】したがって、この発明によれば、記録媒体の駆動手段を持たないデータ端末装置においても、記録媒体から暗号化コンテンツデータを取得し、かつ、暗号化コンテンツデータを再生できる。

【００５７】好ましくは、データ端末装置の再生部は、データ記録装置に対する認証データを保持し、認証データがデータ記録装置において認証されると、データ記録装置からライセンスを取得する。

【００５８】ライセンスを保持するデータ記録装置において、ライセンスの送信を要求する再生部の正当性が確認されると再生部はライセンスを取得する。

【００５９】したがって、この発明によれば、不正な暗号化コンテンツデータの再生を防止できる。

【００６０】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００６１】図１は、本発明によるデータ端末装置（パーソナルコンピュータまたは携帯電話機）がＣＤ－ＲＯＭから暗号化コンテンツデータを取得し、その取得した暗号化コンテンツデータのライセンスを配信サーバから受信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００６２】なお、以下ではインターネットを介して音

楽データを各パーソナルコンピュータのユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００６３】図１を参照して、パーソナルコンピュータ５０は、ＣＤ－ＲＯＭ６０から暗号化音楽データを取得すると、モデム４０およびインターネット網３０を介して、暗号化コンテンツデータを再生するライセンスの配信要求（配信リクエスト）を配信サーバ１０に送信する。著作権の存在する音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来たパーソナルコンピュータのユーザが所有するパーソナルコンピュータ５０が正当な認証データを持つか否か、すなわち、正規のパーソナルコンピュータであるか否かの認証処理を行ない、正当なパーソナルコンピュータに対して所定の暗号方式によりライセンスを暗号化した上で、このような暗号化したライセンスをパーソナルコンピュータ５０に配信する。

【００６４】また、パーソナルコンピュータ５０は、ＣＤ－ＲＯＭ６０から暗号化コンテンツデータを取込み、その取込んだ暗号化コンテンツデータをＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ケーブル７０を介して携帯電話機１００へ送信する。そして、携帯電話機１００は、装着されたメモリカード１１０に暗号化コンテンツデータを記録し、その暗号化コンテンツデータを再生するためのライセンスを、携帯電話網を介して配信サーバ１０へライセンスの配信要求を送信する。そうすると、配信サーバ１０は、メモリカードの正当性を認証データによって確認し、正規のメモリカードからのアクセスであることが判明すれば、携帯電話網を介してライセンスをメモリカード１１０に配信するために、所定の暗号化を施した暗号化ライセンスを通信キャリア２０に渡す。これによって、パーソナルコンピュータ５０から取得した暗号化コンテンツデータを再生するためのライセンスがメモリカード１１０に送信される。携帯電話機１００は、メモリカード１１０に記録された暗号化コンテンツデータをライセンスによって再生するコンテンツ再生デバイス（図示せず）を内蔵しており、携帯電話機１００のユーザは、携帯電話機１００に接続されたヘッドホーン１３０を介してコンテンツ再生デバイスによって再生された音楽を聞くことができる。

【００６５】通常、携帯電話機は、ＣＤ－ＲＯＭから、直接、暗号化コンテンツデータを取得することができないため、パーソナルコンピュータ５０を介してＣＤ－ＲＯＭから暗号化コンテンツデータを取得できる。

【００６６】したがって、図１に示すデータ配信システムにおいては、パーソナルコンピュータ５０は、モデム４０およびインターネット網３０を介して配信サーバ１０からライセンスを受信するとともに、ＣＤ－ＲＯＭ６０から暗号化コンテンツデータを取得する。また、携帯電話機１００に装着されたメモリカード１１０は、パーソナルコンピュータ５０がＣＤ－ＲＯＭ６０から取得した暗号化コンテンツデータを受信し、その暗号化コンテンツデータを再生するライセンスを配信サーバ１０から受信する。携帯電話機１００のユーザは、パーソナルコンピュータ５０を介することによってＣＤ－ＲＯＭから暗号化コンテンツデータを取得することが可能となる。

【００６７】このような構成とすることで、正規なパーソナルコンピュータまたはメモリカードでないと、配信サーバ１０から暗号化コンテンツデータのライセンスを受信することが困難な構成となる。

【００６８】しかも、配信サーバ１０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、パーソナルコンピュータのユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、インターネット網の使用料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００６９】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話またはパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００７０】本発明の実施の形態においては、特に、配信、移動、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機またはパーソナルコンピュータとも言う。以下同じ））に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００７１】なお、以下の説明においては、配信サーバ１０から、各パーソナルコンピュータ等に暗号化コンテンツデータのライセンスを伝送する処理を「配信」と称することとする。

【００７２】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００７３】まず、Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツ

データ｛Ｄｃ｝ＫｃがこのＣＤ－ＲＯＭ６０よりパーソナルコンピュータ５０に取込まれる。

【００７４】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００７５】また、ＣＤ－ＲＯＭ６０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｃ－ｉｎｆがパーソナルコンピュータ５０に取込まれる。

【００７６】さらに、配信サーバ１０からは、暗号化コンテンツデータのライセンスがパーソナルコンピュータ５０またはメモリカード１１０に配信される。また、配信サーバ１０からのライセンス鍵等の配信を特定するための管理コードであるトランザクションＩＤが配信サーバ１０とパーソナルコンピュータ５０との間、または配信サーバ１０と携帯電話機１００との間でやり取りされる。

【００７７】またさらに、ライセンスとしては、ライセンス鍵Ｋｃ、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード、またはライセンス管理デバイス）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍおよびデータ再生端末における再生に関する制御情報である再生制限情報ＡＣｐが存在する。具体的には、アクセス制御情報ＡＣｍはメモリカード、ライセンス管理モジュールおよびライセンス管理モジュールからのライセンス又はライセンス鍵を外部に出力に対するに当たっての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【００７８】以後、トランザクションＩＤとコンテンツＩＤとを併せてライセンスＩＤと総称し、ライセンス鍵ＫｃとライセンスＩＤとアクセス制限情報ＡＣｍと再生制限情報ＡＣｐとを併せて、ライセンスと総称することとする。

【００７９】本発明の実施の形態においては、記録装置（メモリカード、またはライセンス管理デバイス）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【００８０】禁止クラスリスト関連情報には、ライセンスの配信、移動、チェックアウト、チェックイン、および再生が禁止される携帯電話機、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。

【００８１】禁止クラスリストデータＣＲＬは、配信サーバ１０内で管理されるとともに、メモリカード１１０や、パーソナルコンピュータ５０内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際に、パーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）から受取った禁止クラスリストの更新日時を、所有する禁止クラスリストＣＲＬの更新日時と比較して更新されていないと判断されたとき、更新された禁止クラスリストをパーソナルコンピュータに配信する。また、ライセンス管理モジュール、ライセンス管理デバイス、および携帯電話機１００の間でも禁止クラスリストはやり取りされ、そのデータ変更も上述したのと同じである。さらに、禁止クラスリストの変更については、変更点のみを反映した差分データである差分ＣＲＬを配信サーバ１０側より発生して、これに応じてメモリカード、ハードディスク、およびライセンス管理デバイス内の禁止クラスリストＣＲＬに追加する構成とするも可能である。

【００８２】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカードまたはパーソナルコンピュータ内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードまたはパーソナルコンピュータの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードまたはパーソナルコンピュータへのライセンス鍵の供給を禁止する。このため、携帯電話機またはパーソナルコンピュータではコンテンツデータの再生が、メモリカードでは新たなライセンスの取得が行なえなくなる。

【００８３】このように、メモリカードまたはライセンス管理デバイス内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカードにおける禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって制御されるハードディスクでタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なもの

とすることができる。

【００８４】図３は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【００８５】携帯電話機、メモリカード、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス、およびライセンス管理モジュールには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗは携帯電話機に固有の秘密復号鍵Ｋｐｙおよびメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【００８６】また、コンテンツ再生デバイス（携帯電話機）のクラス証明書としてＣｐｙが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてＣｍｗが設けられる。

【００８７】これらのクラス証明書は、コンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【００８８】これらのコンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式または認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で、出荷時にデータ再生デバイス（携帯電話機）、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａは配信システム全体で共通の公開認証鍵である。

【００８９】メモリカード外とメモリカード間でのデータ授受、またはライセンス管理デバイス外とライセンス管理デバイス間でのデータ授受、またはライセンス管理モジュール外とライセンス管理モジュール間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ１０、携帯電話機１００、メモリカード１１０、ライセンス管理デバイス、ライセンス管理モジュールにおいて生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００９０】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、携帯電話機もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００９１】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカード、ライセンス管理デバイス、ライセンス管理モジュールによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００９２】また、メモリカード１１０、ライセンス管理デバイス、およびライセンス管理モジュール内のデータ処理を管理するための鍵として、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールという媒体ごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍｃｘが存在する。

【００９３】図４は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、暗号化コンテンツデータのコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、パーソナルコンピュータの各ユーザごとにライセンス鍵等へのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４に保持されたライセンスによって再生されるコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００９４】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御され

て、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための公開認証鍵を保持する認証鍵保持部３１３と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００９５】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよび再生制限情報ＡＣｍを、復号処理部３２０によって得られたメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号処理部３２６と、暗号処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号処理部３２８とを含む。

【００９６】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００９７】図５は、図１に示したパーソナルコンピュータ５０の構成を説明するための概略ブロック図である。パーソナルコンピュータ５０は、パーソナルコンピュータ５０の各部のデータ授受を行なうためのバスＢＳ２と、インターネット網を介してライセンス管理デバイス５２０またはライセンス管理モジュール５１１に暗号化コンテンツデータのライセンスを配信サーバ１０から受信するために、配信サーバ１０との間でデータの授受を制御するとともに、ＣＤ－ＲＯＭドライブ５４０を介してＣＤ－ＲＯＭから暗号化コンテンツデータを取得する際の制御を行なうためのコントローラ５１０と、配信サーバ１０からのライセンスの受信を行なう際に配信サーバ１０との間で各種の鍵のやり取りを行ない、ＣＤ－ＲＯＭ６０から取得された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス５２０と、コントローラ５１０に含まれ、ＣＤ－ＲＯＭ６０からの暗号化コンテンツデータの取得をプログラムによって実行するコンテンツ管理モジュール５１１とを含む。

【００９８】ライセンス管理デバイス５２０は、暗号化コンテンツデータのライセンスを配信サーバ１０から受信する際のデータの授受をハード的に行ない、受信したライセンスをハード的に管理するものであるため、高いセキュリティレベルでライセンスの受信とライセンスの管理とを行なうことができるものである。

【００９９】パーソナルコンピュータ５０は、さらに、ＣＤ－ＲＯＭドライブ５４０を介してＣＤ－ＲＯＭ６０から取得した暗号化コンテンツデータおよびコンテンツファイルと、ライセンス管理デバイス５２０によって受信した暗号化コンテンツデータのライセンスの格納する領域を指定するためのエントリ番号を暗号化コンテンツデータのファイル名と対応付けて格納するライセンス管理ファイルとを記憶するハードディスク（ＨＤＤ）５３０を含む。なお、コンテンツリストファイルの詳細については後述する。

【０１００】パーソナルコンピュータ５０は、さらに、暗号化コンテンツデータを携帯電話機１００等に通信する際にコントローラ５１０と端子５８０との間でデータの授受を制御するためのＵＳＢインタフェース５５０と、ＣＤ－ＲＯＭ６０からコンテンツデータを取得するためのＣＤ－ＲＯＭドライブ５４０と、ユーザからの指示を入力するためのキーボード５６０と、各種の情報を視覚的にユーザに与えるためのディスプレイ５７０と、ＵＳＢケーブル７０を接続するための端子５８０と、暗号化コンテンツデータをライセンスによって再生するためのコンテンツ再生デバイス１５５０とを含む。

【０１０１】このように、パーソナルコンピュータ５０は、配信サーバ１０からインターネット網３０を介してライセンスを受信するためのライセンス管理デバイス５２０と、ＣＤ－ＲＯＭ６０から暗号化コンテンツデータを取得するためのＣＤ－ＲＯＭドライブ５４０とを内蔵するものである。

【０１０２】図６は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【０１０３】携帯電話機１００は、携帯電話機１００の各部のデータ授受を行なうためのバスＢＳ３と、携帯電話網により無線伝送される信号を受信するためのアンテナ１０２と、アンテナ１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナに与えるための送受信部１０４と、バスＢＳ３を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、外部からの指示を携帯電話機１００に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【０１０４】携帯電話機１００は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ３との間のデータの授受を制御するためのメモリインタフェース１２００

と、パーソナルコンピュータ５０から暗号化コンテンツデータおよびライセンスを受信する際にバスＢＳ３と端子１１１４との間のデータ授受を制御するためのＵＳＢインタフェース１１１２と、ＵＳＢケーブル７０を接続するための端子１１１４とを含む。

【０１０５】携帯電話機１００は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１を公開復号鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを保持する認証データ保持部１５００を含む。ここで、携帯電話機（データ端末装置）１００のクラスｙは、ｙ＝１であるとする。

【０１０６】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生デバイス）固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１５０２と、バスＢＳ３から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【０１０７】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ３上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃおよび再生制限情報ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化しバスＢＳ３に出力する暗号処理部１５０６とを含む。

【０１０８】携帯電話機１００は、さらに、バスＢＳ３上のデータをセッションキーＫｓ３によって復号して、コンテンツ鍵Ｋｃおよび再生制限情報ＡＣｐを出力する復号処理部１５１０と、バスＢＳ３より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０より取得したライセンス鍵Ｋｃによって復号しコンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【０１０９】なお、図７においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス１５５０を構成する。また、図７においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【０１１０】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１１１】図７は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、これらは自然数ｗ＝３でそれぞれ表わされるものとする。

【０１１２】したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵であるＫｍｃ４を保持するＫｍｃ保持部１４０２と、メモリカードの種類ごとに設定される固有の秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、Ｋｍｃ４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａとして保持する。

【０１１３】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【０１１４】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ４と、バスＢＳ４にインタフェース１４２４から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Ｋｍ３をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から認証鍵ＫＰａを受けて、バスＢＳ４に与えられるデータからＫＰａによる復号処理を実行して復号結果を暗号処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号処理部１４０６とを含む。

【０１１５】メモリカード１１０は、さらに、再生セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐｙもしくはＫＰ

mwによって暗号化してバスＢＳ４に送出する暗号処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生期限ＡＣｐを、復号処理部１４１２で復号されたメモリカード１１０に固有の公開暗号鍵ＫＰｍｃｘで暗号化する暗号処理部１４１７とを含む。

【０１１６】メモリカード１１０は、さらに、バスＢＳ４上のデータを公開暗号鍵ＫＰｍｃ４と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、禁止クラスリストデータＣＲＬと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ）と、付加情報Ｄａｔａ－ｉｎｆと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１５１５は、禁止クラスリストＣＲＬを記録したＣＲＬ領域１４１５Ａと、ライセンスを記録したライセンス領域１４１５Ｂと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータの関連情報Ｄｃ－ｉｎｆ、再生リスト、およびライセンス管理ファイルを記録したデータ領域１４１５Ｃとから成る。

【０１１７】ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【０１１８】また、ライセンス領域１４１５Ｂは、ライセンス（コンテンツ鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ）を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【０１１９】メモリカード１１０は、さらに、バスＢＳ４を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１２０】なお、データ領域１４１５Ｃを除く全ての構成は、耐タンパモジュール領域に構成される。

【０１２１】以降では、簡単化のためアクセス制御情報ＡＣｍは再生回数の制限を行なう制御情報である再生回数のみを、再生回路制御情報ＡＣｐは再生可能な期限を規定する制御情報である再生期限のみを制限するものとし、アクセス制御情報ＡＣｍおよび再生回路制御情報ＡＣｐを、それぞれ、再生回数制限ＡＣｍ、再生期限ＡＣｐと称するものとする。

【０１２２】図８は、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０の構成を示す概略ブロック図である。ライセンス管理デバイス５２０は、基本的にメモリカード１１０と同じ構成から成る。ライセンス管理デバイス５２０の認証データ保持部５２００、Ｋｍｃ保持部５２０２、復号処理部５２０４、暗号処理部５２０６、復号処理部５２０８、暗号処理部５２１０、復号処理部５２１２、ＫＰａ保持部５２１４、ＫＰｍｃ保持部５２１６、暗号処理部５２１７、セッションキー発生部５２１８、コントローラ５２２０、Ｋｍ保持部５２２１、復号処理部５２２２、インタフェース５２２４、端子５２２６、切換スイッチ５２４２，５２４６は、それぞれ、メモリカード１１０の認証データ保持部１４００、Ｋｍｃ保持部１４０２、復号処理部１４０４、暗号処理部１４０６、復号処理部１４０８、暗号処理部１４１０、復号処理部１４１２、ＫＰａ保持部１４１４、ＫＰｍｃ保持部１４１６、暗号処理部１４１７、セッションキー発生部１４１８、コントローラ１４２０、Ｋｍ保持部１４２１、復号処理部１４２２、インタフェース１４２４、端子１４２６、切換スイッチ１４４２，１４４６と同じである。ただし、認証データ保持部５２００は、｛ＫＰｍ７／／Ｃｍ７｝ＫＰａの形式で認証データを保持し、Ｋｍ保持部５２０２は、秘密復号鍵Ｋｍ７を保持し、Ｋｍｃ保持部５２２１は、秘密復号鍵Ｋｍｃ８を保持する。

【０１２３】ライセンス管理デバイス５２０は、禁止クラスリストＣＲＬとライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ）とを記録するメモリ５２１５を、メモリカード１１０のメモリ１４１５に代えて含む。メモリ５２１５は、禁止クラスリストＣＲＬを記録したＣＲＬ領域５２１５Ａと、ライセンスを記録したライセンス領域５２１５Ｂとから成る。

【０１２４】以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【０１２５】［配信］次に、図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理デバイス５２０へ暗号化コンテンツデータのライセンスを配信する動作について説明する。

【０１２６】図９～図１３は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０への配信動作（以下、配信セッションともいう）を説明するための第１～第５のフローチャートである。

【０１２７】図９を参照して、パーソナルコンピュータ５０のユーザからキーボード５６０を介してＣＤ－ＲＯＭ６０から暗号化コンテンツデータを取得する指示が入力されると、パーソナルコンピュータ５０のコントロー

ラ５１０は、ＣＤ－ＲＯＭに記録されたコンテンツリストに従って、コンテンツデータのリストを作成し、ライセンスの購入要求の確認を行なう（ステップＳ７８）。そして、コンテンツＩＤの指定による配信リクエストがなされ（ステップＳ８０）、キーボード５６０を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ８２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータの再生回数制限ＡＣｍ、および再生期限ＡＣｐを設定して購入条件ＡＣが入力される。

【０１２８】暗号化コンテンツデータの購入条件ＡＣが入力されると、ＣＤ－ＲＯＭからサーバ情報ファイルが取得されたか否かが判別され（ステップＳ８４）、サーバ情報ファイルが取得されなかったときはステップＳ１００へ移行し、サーバ情報ファイルが取得されたときは、次のステップＳ８６へ移行する（ステップＳ８４）。

【０１２９】ステップＳ８４において、サーバ情報ファイルが取得されたと判別されると、配信リクエストされたコンテンツに対する情報の有無が判別される（ステップＳ８６）。つまり、「このコンテンツデータを取得するためには、インターネットを用いなさい。」とか、「このコンテンツデータを取得するためには、電話回線を用いなさい。」とかのようにＣＤ－ＲＯＭ６０から取得された暗号化コンテンツデータの種類に応じて配信サーバ１０に接続するための接続手段に関する情報や、「このコンテンツに対しては、どこのサーバへアクセスしなさい」とかのライセンスを取得するためにアクセスすべきアドレス等の情報の有無を判別する。そして、ステップＳ８６において、このような情報がないときは、ステップＳ１００へ移行し、情報があるときは、ステップＳ８８へ移行する。

【０１３０】ステップＳ８６において、コンテンツデータに対する情報が有ると判別されると、配信サーバ１０との接続方法の確認が成される（ステップＳ８８）。つまり、インターネットによって接続するのか、電話回線によって接続するのか、それとも、インターネットおよび電話回線で接続しないのかの確認が行われる。そして、電話回線で接続するときは、ステップＳ９０へ移行し、インターネットによって接続するときはステップＳ９４へ移行し、インターネットおよび電話回線で接続できないときはステップＳ１９０へ移行して配信セッションは終了する。

【０１３１】ステップＳ８８において電話回線によって接続することが確認されると、サーバ情報ファイルから電話番号が取得され（ステップＳ９０）、取得した電話番号をダイヤルしてモデム経由で配信サーバ１０に接続する（ステップＳ９２）。一方、ステップＳ８８において、インターネットによって接続することが確認されると、回線が接続されたか否かの確認が行われ（ステップＳ９４）、未接続のときはステップＳ１９０へ移行して配信セッションは終了し、回線の接続が確認されたときはステップＳ９６へ移行する（ステップＳ９４）。

【０１３２】ステップＳ９４において、回線に接続が確認されると、サーバ情報ファイルからＵＲＬが取得され（ステップＳ９６）、ＵＲＬに基づいて配信サーバ１０と接続される（ステップＳ９８）。また、ステップＳ８４にサーバ情報ファイルが無いと判別されたとき、またはステップＳ８６においてコンテンツデータに対する情報が無いと判別されたとき、ユーザによって配信サーバ１０との接続が指示され（ステップＳ１００）、配信サーバ１０との接続が確認される（ステップＳ１０２）。ステップＳ１０２において、未接続と判別されるとステップＳ１９０へ移行して配信セッションは終了し、接続と判別されると、次のステップＳ１０４へ移行する。

【０１３３】図１０を参照して、ステップＳ９２またはステップＳ９８またはステップＳ１０２の後、コントローラ５１０は、バスＢＳ２を介してライセンス管理デバイス５２０へ認証データの出力指示を与える（ステップＳ１０４）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して認証データの出力指示を受取る。そして、コントローラ５２２０は、バスＢＳ５を介して認証データ保持部５２００から認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａを読出し、｛ＫＰｍ７／／Ｃｍ７｝ＫＰａをバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ１０６）。

【０１３４】パーソナルコンピュータ５０のコントローラ５１０は、ライセンス管理デバイス５２０からの認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１０８）。

【０１３５】配信サーバ１０では、パーソナルコンピュータ５０から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１０）、復号処理部３１２においてライセンス管理デバイス５２０から出力された認証データを公開認証鍵ＫＰａで復号処理を実行する（ステップＳ１１２）。

【０１３６】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、ライセンス管理デバイス５２０が正規のライセンス管デバイスからの公開暗号鍵ＫＰｍ７と証明書Ｃｍ７とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１４）。正当な認証データであると判断された

場合、配信制御部３１５は、公開暗号鍵ＫＰｍ７および証明書Ｃｍ７を承認し、受理する。そして、次の処理（ステップＳ１１６）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍ７および証明書Ｃｍ７を受理しないで処理を終了する（ステップＳ１９８）。

【０１３７】認証の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、ライセンス管理デバイスのクラス証明書Ｃｍ７が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１９８）。

【０１３８】一方、ライセンス管理デバイス５２０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１６）。

【０１３９】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ１０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１８）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１２０）。セッションキーＫｓ１は、復号処理部３１２によって得られたライセンス管理デバイス５２０に対応する公開暗号鍵ＫＰｍ７によって、暗号処理部３１８によって暗号化される（ステップＳ１２２）。

【０１４０】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ//｛Ｋｓ１｝Ｋｍ７として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０１４１】図１１を参照して、パーソナルコンピュータ５０が、トランザクションＩＤ//｛Ｋｓ１｝Ｋｍ７を受信すると（ステップＳ１２６）、コントローラ５１０は、トランザクションＩＤ//｛Ｋｓ１｝Ｋｍ７をライセンス管理デバイス５２０に入力する（ステップＳ１２８）。そうすると、ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、バスＢＳ５に与えられた受信データを、復号処理部５２２２が、保持部５２２１に保持されるライセンス管理デバイス５２０に固有の秘密復号鍵Ｋｍ７により復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３０）。

【０１４２】コントローラ５２２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部５２１８に対してライセンス管理デバイス５２０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部５２１８は、セッションキーＫｓ２を生成する（ステップＳ１３２）。

【０１４３】また、配信セッションにおいては、コントローラ５２２０は、ライセンス管理デバイス５２０内のメモリ５２１５に記録されている禁止クラスリストの更新日時ＣＲＬｄａｔｅをメモリ１４１５から抽出して切換スイッチ５２４６に出力する（ステップＳ１３４）。

【０１４４】暗号処理部５２０６は、切換スイッチ５２４２の接点Ｐａを介して復号処理部５２２２より与えられるセッションキーＫｓ１によって、切換スイッチ５２４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍｃ８および更新日時ＣＲＬｄａｔｅを１つのデータ列として暗号化して、｛Ｋｓ２//ＫＰｍｃ８//ＣＲＬｄａｔｅ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１３６）。

【０１４５】バスＢＳ３に出力された暗号化データ｛Ｋｓ２//ＫＰｍｃ８//ＣＲＬｄａｔｅ｝Ｋｓ１は、バスＢＳ３からインタフェース５２２４および端子５２２６を介してパーソナルコンピュータ５０に出力され、パーソナルコンピュータ５０から配信サーバ１０に送信される（ステップＳ１３８）。

【０１４６】配信サーバ１０は、トランザクションＩＤ//｛Ｋｓ２//ＫＰｍｃ８//ＣＲＬｄａｔｅ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、ライセンス管理デバイス５２０で生成されたセッションキーＫｓ２、ライセンス管理デバイス５２０固有の公開暗号鍵ＫＰｍｃ８およびライセンス管理デバイス５２０における禁止クラスリストの更新日時ＣＲＬｄａｔｅを受理する（ステップＳ１４２）。

【０１４７】配信制御部３１５は、ステップＳ１１０で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐを生成する（ステップＳ１４４）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１４６）。

【０１４８】配信制御部３１５は、生成したライセンス、すなわち、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生期限ＡＣｐ、およびアクセス制限情報ＡＣｍを暗号処理部３２６に与える。暗号処理部３２６は、復号処理部３２０によって得られたライセンス管理デバイス５２０固有の公開暗号鍵ＫＰｍｃ８によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ｝Ｋｍｃ８を生成する（ステップＳ１４８）。

【０１４９】図１２を参照して、配信サーバ１０において、ライセンス管理デバイス５２０から送信された禁止クラスリスト更新日時ＣＲＬｄａｔｅから、ライセンス

管理デバイス５２０が保持する禁止クラスリストＣＲＬが最新か否かが判断され、最新と判断されたとき、ステップＳ１５２へ移行する。最新でないときはステップＳ１６０へ移行する（ステップＳ１５０）。

【０１５０】最新と判断されたとき、暗号処理部３２８は、暗号処理部３２６から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８をライセンス管理デバイス５２０において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を通信装置３５０を介してパーソナルコンピュータ５０へ送信する（ステップＳ１５２）。

【０１５１】そして、パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し（ステップＳ１５４）、バスＢＳ５を介してライセンス管理デバイス５２０に入力する。ライセンス管理デバイス５２０の復号処理部５２１２は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を端子５２２６およびインタフェース５２２４を介して受取り、セッションキー発生部５２１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８を受理する（ステップＳ１５８）。その後、ステップＳ１７２へ移行する。

【０１５２】一方、最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストのデータＣＲＬｄａｔｅを取得し、差分データである差分ＣＲＬを生成する（ステップＳ１６０）。

【０１５３】暗号処理部３２８は、暗号処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの差分ＣＲＬとを受けて、ライセンス管理デバイス５２０において生成されたセッションキーＫｓ２によって暗号化する。暗号処理部３２８より出力された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２は、バスＢＳ１および通信装置３５０を介してパーソナルコンピュータ５０に送信される（ステップＳ１６２）。

【０１５４】パーソナルコンピュータ５０は、送信された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝Ｋｓ２を受信し（ステップＳ１６４）、バスＢＳ５を介してライセンス管理デバイス５２０に入力する（ステップＳ１６６）。ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、バスＢＳ５に与えられた受信データを復号処理部５２１２によって復号する。復号処理部５２１２は、セッションキー発生部５２１８から与えられたセッションキーＫｓ２を用いてバスＢＳ５の受信データを復号しバスＢＳ５に出力する（ステップＳ１６８）。

【０１５５】この段階で、バスＢＳ５には、Ｋｍｃ保持部５２２１に保持される秘密復号鍵Ｋｍｃ８で復号可能な暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８｝と、差分ＣＲＬとが出力される（ステップＳ１６８）。コントローラ５２２０の指示によって受理した差分ＣＲＬによってメモリ５２１５内のＣＲＬ領域５２１５Ａを差分ＣＲＬに基づいて更新する（ステップＳ１７０）。

【０１５６】ステップＳ１５２，Ｓ１５４，Ｓ１５６，Ｓ１５８は、ライセンス管理デバイス５２０の禁止クラスリストＣＲＬが最新の場合のライセンス鍵Ｋｃ等のライセンス管理デバイス５２０への配信動作であり、ステップＳ１６０，Ｓ１６２，Ｓ１６４，Ｓ１６６，Ｓ１６８，Ｓ１７０は、ライセンス管理デバイス５２０の禁止クラスリストＣＲＬが最新でない場合のライセンス鍵Ｋｃ等のライセンス管理デバイス５２０への配信動作である。このように、ライセンス管理デバイス５２０から送られてきた禁止クラスリストＣＲＬｄａｔｅが更新されているか否かを、逐一、確認し、最新の禁止クラスリストＣＲＬをＣＲＬデータベース３０６から取得し、差分ＣＲＬをライセンス管理デバイス５２０に配信することによって、配信したライセンスが、クラス鍵等の破られた機器に対して出力され、流出することを防止できる。

【０１５７】ステップＳ１５８またはステップＳ１７０の後、コントローラ５２２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８は、復号処理部５２０４において、秘密復号鍵Ｋｍｃ８によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、再生回数制限ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ１７２）。

【０１５８】このように、配信サーバおよびライセンス管理デバイスでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０１５９】図１３を参照して、コントローラ５１０は、ライセンス管理デバイス５２０が受理したライセンスを格納するためのエントリ番号を、ライセンス管理デバイス５２０に入力する（ステップＳ１７４）。そうす

ると、ライセンス管理デバイス５２０のコントローラ５２０は、端子５２２６およびインタフェース５２２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ５２１５のライセンス領域５２１５Ｂに、ステップＳ１７２において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、再生回数制限ＡＣｍおよび再生期限ＡＣｐ）を格納する（ステップＳ１７６）。

【０１６０】パーソナルコンピュータ５０のコントローラ５１０は、配信サーバ１０から送られたトランザクションＩＤと、ライセンスの配信受理を配信サーバ１０へ送信する（ステップＳ１７８）。

【０１６１】配信サーバ１０は、トランザクションＩＤおよびライセンスの配信受理を受信し（ステップＳ１８０）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行われる（ステップＳ１８２）。

【０１６２】一方、パーソナルコンピュータ５０においては、ステップＳ１７８の後、ライセンスのエントリ番号、トランザクションＩＤ、およびコンテンツＩＤを含むライセンス管理ファイルを生成し、ＨＤＤ５３０に記録する（ステップＳ１８４）。そして、コントローラ５１０は、ＣＤ－ＲＯＭドライブ５４０がＣＤ－ＲＯＭから読出したコンテンツファイル（｛Ｄｃ｝Ｋｃ，Ｄｃ－ｉｎｆ）をＨＤＤ５３０にコピーし（ステップＳ１８６）、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツを追記し（ステップＳ１８８）、全体の動作が終了する。

【０１６３】このようにして、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５０が正規の機器であること、同時に、クラス証明書Ｃｍ７とともに暗号化して送信できた公開暗号鍵ＫＰｍ７が有効であることを確認した上で、クラス証明書Ｃｍ７が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ７による暗号化が破られたクラス証明書リストに記載されていないライセンス管理デバイスからの配信要求に対してのみコンテンツデータのライセンスを配信することができ、不正なライセンス管理デバイスへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１６４】なお、パーソナルコンピュータ５０からＵＳＢケーブル７０を介してＣＤ－ＲＯＭ６０から取得された暗号化コンテンツデータを受信し、メモリカード１１０に暗号化コンテンツデータを記録した携帯電話機１００は、上記図９～図１３に示すフローチャートに従って、配信サーバ１０から携帯電話網を介してライセンスを受信してメモリカード１１０に記録する。ただし、携帯電話機１００が配信サーバ１０からライセンスを受信するときは、パーソナルコンピュータ５０を介したＣＤ－ＲＯＭ６０からの暗号化コンテンツデータの取得が最初に行われる。この場合は、最初に暗号化コンテンツデータを受信しないと、携帯電話機１００は、サーバ情報ファイルを取得できず、アクセスすべき配信サーバや、配信サーバとの接続手段が解らないからである。

【０１６５】［移動］図１に示すデータ配信システムにおいて、ＣＤ－ＲＯＭ６０から取得された暗号化コンテンツデータと、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理デバイス５２０へ配信された暗号化コンテンツデータのライセンスを携帯電話機１００に装着されたメモリカード１１０へ送信する動作について説明する。なお、この動作を「移動」という。

【０１６６】図１４～図１７は、図１に示すデータ配信システムにおいて、ライセンス管理デバイス５２０が配信サーバ１０から受信した暗号化コンテンツデータのライセンスと、ＣＤ－ＲＯＭ６０から取得した暗号化コンテンツデータを携帯電話機１００に装着されたメモリカード１１０へ移動する移動動作を説明するための第１～第４のフローチャートである。

【０１６７】図１４を参照して、パーソナルコンピュータ５０のキーボード５６０から移動リクエストが入力されると（ステップＳ３００）、コントローラ５１０は、認証データの送信要求をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して携帯電話機１００へ送信する（ステップＳ３０２）。そうすると、携帯電話機１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２およびバスＢＳ３を介して認証データの送信要求を受信し、バスＢＳ３およびメモリカードインタフェース１２００を介して認証データの送信要求をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ３０４）。

【０１６８】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して携帯電話機１００へ出力する。そして、携帯電話機１００のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ３０６）。

【０１６９】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し（ステップＳ３０８）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢ

Ｓ２を介してライセンス管理デバイス５２０へ送信する。ライセンス管理デバイス５２０のコントローラ５２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを復号処理部５２０８へ与える。認証処理部５２０８は、ＫＰａ保持部５２１４からの認証鍵ＫＰａによって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａの復号処理を実行する（ステップＳ３１０）。コントローラ５２２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍ３と証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ３１２）。正当な認証データであると判断された場合、コントローラ５２２０は、公開暗号鍵ＫＰｍ３および証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ３１４）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍ３および証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ４０４）。

【０１７０】認証の結果、正規のメモリカードであることが認識されると、コントローラ５２２０は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをメモリ５２１５のＣＲＬ領域５２１５Ａに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する（ステップＳ４０４）。

【０１７１】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ３１４）。

【０１７２】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス５２０において、コントローラ５２２０は、移動を特定するための管理コードであるトランザクションＩＤをメモリ５２１５のライセンス領域５２１５Ｂから取得する（ステップＳ３１６）。そして、セッションキー発生部５２１８は、移動のためのセッションキーＫｓ２２を生成する（ステップＳ３１８）。セッションキーＫｓ２２は、復号処理部５２０８によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍ３によって、暗号処理部５２１０によって暗号化される（ステップＳ３２０）。コントローラ５２２０は、バスＢＳ５を介して暗号化データ｛Ｋｓ２２｝Ｋｍ３を取得し、メモリ５２１５から取得したトランザクションＩＤを暗号化データ｛Ｋｓ２２｝Ｋｍ３に追加したトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ３２２）。

【０１７３】図１５を参照して、パーソナルコンピュータ５０のコントローラ５１０は、バスＢＳ２を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し（ステップＳ３２４）、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を携帯電話機１００へ送信する（ステップＳ３２４）。そうすると、携帯電話機１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびＢＳ３を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し、その受信したトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信する（ステップＳ３２６）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２２｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からの秘密復号鍵Ｋｍ３によって｛Ｋｓ２２｝Ｋｍ３を復号してセッションキーＫｓ２２を受理する（ステップＳ３２８）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成し（ステップＳ３３０）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ３３２）。

【０１７４】そうすると、暗号処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２、公開暗号鍵ＫＰｍｃ４および禁止クラスリストＣＲＬｄａｔｅを、復号処理部１４０４によって復号されたセッションキーＫｓ２２によって暗号化し、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して携帯電話機１００へ出力し、携帯電話機１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受取る。そして、コントローラ１１０６は、ＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ３３４）。

【０１７５】パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／

CRLdate}Ks22を受信し（ステップS336）、バスBS2を介して暗号化データ{Ks2//KPmc4//CRLdate}Ks22をライセンス管理デバイス520へ入力する（ステップS338）。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS5を介して暗号化データ{Ks2//KPmc4//CRLdate}Ks22を受信し、その受信した暗号化データ{Ks2//KPmc4//CRLdate}Ks22を復号処理部5212に与える。復号処理部5212は、セッションキー発生部5218からのセッションキーKs22によって暗号化データ{Ks2//KPmc4//CRLdate}Ks22を復号し、セッションキーKs2、公開暗号鍵KPmc4および禁止クラスリストの更新日時CRLdateを受理する（ステップS340）。

【0176】そうすると、パーソナルコンピュータ50のコントローラ510は、ステップS324においてライセンス管理デバイス520から取得したトランザクションIDに基づいて、HDD530に記録されたコンテンツリストファイルに含まれるライセンス管理ファイルを検索し、取得したトランザクションIDが含まれるライセンス管理ファイルと同じライセンス管理ファイルに含まれるライセンスのエントリ番号をHDD530から読出す。そして、コントローラ510は、その読出したエントリ番号をバスBS2を介してライセンス管理デバイス520に入力する（ステップS342）。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介してエントリ番号を受信し、メモリ5215のライセンス領域5215Bにおいて受信したエントリ番号によって指定された領域からトランザクションID、コンテンツID、ライセンス鍵Kc、再生回数制限ACm、再生期限ACpを読出す（ステップS344）。

【0177】再生回数制限ACmの受理に応じて、コントローラ5220は、再生回数制限ACmを確認する（ステップS346）。つまり、コントローラ5220は、取得した再生回数制限ACmに基づいて、携帯電話機100に装着されたメモリカード110へ移動しようとするライセンスが再生回数制限ACmによって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数が再生回数制限ACmによる制限回数に達している場合、暗号化コンテンツデータをライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとを携帯電話機100に装着されたメモリカード110へ移動する意味がないからである。

【0178】ステップS346において、暗号化コンテンツデータの再生回数が再生回数制限ACmによる制限回数に達していた場合、ステップS404へ移行し、移動動作は終了する。ステップS346において、暗号化コンテンツデータの再生回数が再生回数制限ACmによる制限回数に達していない場合、ステップS348へ移行する。

【0179】図16を参照して、暗号処理部5217は、復号処理部5212によって得られたライセンス管理デバイス520固有の公開暗号鍵KPmc4によってライセンスを暗号化して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4を生成する（ステップS348）。そして、メモリカード110から送信された禁止クラスリストの更新日時CRLdateによって、メモリカード110とライセンス管理デバイス320の保持する禁止クラスリストCRLのいずれが新しいかが判断され、メモリカード110が保持する禁止クラスリストが新しいか同じと判断されたとき、ステップS350へ移行する。また、ライセンス管理デバイス520が保持する禁止クラスリストが最新でないときはステップS362へ移行する（ステップS350）。

【0180】メモリカード110の方が新しい、もしくは、同じと判断されたとき、暗号処理部5206は、暗号処理部5217から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4をセッションキー発生部5218において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2をバスBS5に出力する。そして、コントローラ5220は、バスBS5上の暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2をインタフェース5224および端子5226を介してパーソナルコンピュータ50へ送信する（ステップS352）。そして、コントローラ5220は、メモリ5215のライセンス領域5215Bにおいて指定されたエントリ番号内のライセンスを削除する（ステップS354）。

【0181】パーソナルコンピュータ50のコントローラ510は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を受取り、USBインタフェース550、端子580、およびUSBケーブル70を介して携帯電話機100へ送信する（ステップS356）。

【0182】携帯電話機100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を受信し、その受信した暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2をバスBS3およびメモリカードインタフェース1200を介

してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、端子１４２４、およびバスＢＳ４を介して暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ３５８）。

【０１８３】メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ３６０）。その後、図１７に示すステップＳ３７６へ移行する。

【０１８４】一方、ステップＳ３５０において、ライセンス管理デバイスの方が新しいと判断されると、ライセンス管理デバイス５２０のコントローラ５２２０は、バスＢＳ５を介してメモリ５２１５のＣＲＬ領域５２１５Ａから最新の禁止クラスリストのデータＣＲＬを取得する（ステップＳ３６２）。

【０１８５】暗号処理部５２０６は、暗号処理部５２１７の出力と、コントローラ５２２０がバスＢＳ５を介してメモリ５２１５から取得した禁止クラスリストのデータＣＲＬとを、それぞれ、切換スイッチ５２４２および５２４６を介して受取り、セッションキー発生部５２１８において生成されたセッションキーＫｓ２によって暗号化する。暗号処理部５２０６より出力された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／インタフェース５２２４、および端子５２２６を介してパーソナルコンピュータ５０に出力される（ステップＳ３６４）。そして、コントローラ５２２０は、メモリ５２１５のライセンス領域５２１５Ｂにおける指定されたエントリ番号内のライセンスを削除する（ステップＳ３６６）。

【０１８６】このように、ライセンス管理デバイスおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスの移動動作におけるセキュリティを向上させることができる。

【０１８７】パーソナルコンピュータ５０のコントローラ５１０は、出力された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を携帯電話機１００へ送信する（ステップＳ３６８）。携帯電話機１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受取り、バスＢＳ３およびメモリカードインタフェース１２００を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ３７０）。

【０１８８】メモリカード１１０において、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ４上の受信データを復号し、ＣＲＬと｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４とを受理する（ステップ３７２）。コントローラ１４２０は、復号処理部１４１２によって受理されたデータＣＲＬをバスＢＳ４を介して受取り、その受取ったデータＣＲＬによってメモリ１４１５のＣＲＬ領域１４１５Ａを書換える（ステップＳ３７４）。

【０１８９】ステップＳ３５２，Ｓ３５４，Ｓ３５６，Ｓ３５８，Ｓ３６０は、メモリカード１１０の保持する禁止クラスリストＣＲＬが、ライセンス管理デバイス５２０の禁止クラスリストＣＲＬより新しいか、同じ場合のライセンス鍵Ｋｃ等のメモリカード１１０への移動動作であり、ステップＳ３６２，Ｓ３６４，Ｓ３６６，Ｓ３６８，Ｓ３７０，Ｓ３７２，Ｓ３７４は、メモリカード１１０の保持する禁止クラスリストＣＲＬが、ライセンス管理デバイス５２０の禁止クラスリストＣＲＬより古い場合のライセンス鍵Ｋｃ等のメモリカード１１０への移動動作である。このように、メモリカード１１０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅに従って、、逐一、確認し、より最新の禁止クラスリストＣＲＬに更新される。を防止できる。

【０１９０】図１７を参照して、ステップＳ３６０またはステップＳ３７４の後、コントローラ１４２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、再生回数制限ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ３７６）。

【０１９１】パーソナルコンピュータ５０のコントロー

ラ５１０は、メモリカード１１０へ移動したライセンスを格納するためのエントリ番号を、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して携帯電話機１００へ送信し、携帯電話機１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、バスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する（ステップＳ３７８）。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ３７６において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、再生回数制限ＡＣｍおよび再生期限ＡＣｐ）を格納する（ステップＳ３８０）。

【０１９２】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０のメモリ１４１５に格納されたライセンスのエントリ番号と、平文のトランザクションＩＤおよびコンテンツＩＤを含むメモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、メモリカード１１０へ送信する（ステップＳ３８２）。

【０１９３】メモリカード１１０のコントローラ１４２０は、携帯電話機１００を介してライセンス管理ファイルを受信し、メモリ１４１５のデータ領域１４１５Ｄに受信したライセンス管理ファイルを記録する（ステップＳ３８４）。

【０１９４】そして、パーソナルコンピュータ５０のコントローラ５１０は、ＨＤＤ５３０に記録されたライセンスのうち、メモリカード１１０へ移動したライセンスに対するライセンス管理ファイルをライセンス無に更新する（ステップＳ３８６）。その後、コントローラ５１０は、メモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとをＨＤＤ５３０から取得し、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリカード１１０へ送信する（ステップＳ３９０）。メモリカード１１０のコントローラ１４２０は、携帯電話機１００を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信し（ステップＳ３９２）、バスＢＳ４を介して受信した｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ３９４）。

【０１９５】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０へ移動した楽曲を追記した再生リストを作成し（ステップＳ３９６）、再生リストと、再生リストの書換指示とをメモリカード１１０へ送信する（ステップＳ３９８）。メモリカード１１０のコントローラ１４２０は、携帯電話機１００を介して再生リストと書換指示とを受信し（ステップＳ４００）、バスＢＳ４を介してメモリ１４１５のデータ領域１４１５Ｃに記録されている再生リストを受信した再生リストに書換え（ステップＳ４０２）、移動動作が終了する（ステップＳ４０４）。

【０１９６】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上で、クラス証明書Ｃｍ３が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ３による暗号化が破られたクラス証明書リストに記載されていないメモリカードへの移動要求に対してのみコンテンツデータを移動することができ、不正なメモリカードへの移動および解読されたクラス鍵を用いた移動を禁止することができる。また、この移動動作を用いることによって、配信サーバ１０との通信機能を有さない携帯電話機１０２のユーザも、パーソナルコンピュータ５０を介して暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【０１９７】なお、上記においては、パーソナルコンピュータ５０のライセンス管理デバイス５２０からメモリカード１１０へのライセンスの移動について説明したが、メモリカード１１０からライセンス管理デバイス５２０へのライセンスの移動も、図１４～図１７に示すフローチャートに従って行なわれる。

【０１９８】図１８を参照して、パーソナルコンピュータ５０のライセンス管理デバイス５２０によって受信されたライセンスの管理について説明する。パーソナルコンピュータ５０のＨＤＤ５３０は、コンテンツリストファイル１５０と、コンテンツファイル１５３１～１５３ｎと、ライセンス管理ファイル１５２１～１５２ｎとを含む。

【０１９９】コンテンツリストファイルは、ＨＤＤ５３０に記録されているコンテンツを管理するためのファイルで、コンテンツの一覧と、対応するコンテンツファイルとライセンス管理ファイルへの関係を示す情報ファイルである。

【０２００】コンテンツファイル１５３１～１５３ｎは、ＣＤ－ＲＯＭから取得された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとが記録されたファイルである。なお、コンテンツファイル１５３１～１５３ｎは、ＣＤ－ＲＯＭに記録されているコンテンツファイル６０１～６０ｎのコピーである。また、ライセンス管理ファイル１５２１～１５２ｎは、それぞれ、コンテンツファイル１５３１～１５３ｎに対応して記録されており、ライセンス管理デバイス５２０によって受信されたライセンスを管理する。

【０２０１】ライセンス管理ファイル１５２１，１５２

4は、それぞれ、エントリ番号0，2を含む。これは、ライセンス管理デバイス５２０によって受信され、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ｂにおいて管理されるライセンス（ライセンスＩＤ、ライセンス鍵Ｋｃ、再生回数制限ＡＣｍおよび再生期限ＡＣｍ）の管理領域を指定する番号である。

【０２０２】したがって、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを携帯電話機１００に装着されたメモリカード１１０へ移動させるとき、コンテンツファイル１５３１～１５３ｎを検索してコンテンツファイル１５３１を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル１５３１に対応するライセンス管理ファイル１５２１に含まれるエントリ番号は「0」であるので、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ｂのエントリ番号0によって指定された領域に記録されている。そうすると、ＨＤＤ５３０に記録されたコンテンツリストファイル１５０のライセンス管理ファイル１５２１からエントリ番号0を読出し、その読出したエントリ番号0をライセンス管理デバイス５２０に入力することによって、メモリ５２１５のライセンス領域５２１５Ｂからライセンスを容易に取出し、メモリカード１１０へ移動できる。そして、ライセンスを移動した後、ライセンスの複製が禁止されているとき、メモリ５２１５のライセンス領域５２１５Ｂにおいて指定されたエントリ番号0内のライセンスは削除されるので、それに対応してライセンス管理ファイル１５２３のように「ライセンス無」が記録される。

【０２０３】図１９は、メモリカード１１０のメモリ１４１５におけるデータ領域１４１５Ｃに記録された再生リストファイル１６０と、コンテンツファイル１６１１～１６１ｎと、ライセンス管理ファイル１６２１～１６２ｎとの関係を示したものである。再生リスト１６０は、パーソナルコンピュータ５０におけるコンテンツリストファイル１５０に相当する情報リストであり、携帯電話機１００ではこの再生リストを参照して、通常、リスト順に再生していく。コンテンツファイル１６１１～１６１ｎは、受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとのファイル名を記録する。また、ライセンス管理ファイル１６２１～１６２ｎは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記録されている。

【０２０４】また、ライセンス管理ファイル１６２１～１６２ｎは、メモリ１４１５のライセンス領域１４１５Ｃに格納されたライセンスの領域を指定するためのエントリ番号を含む。したがって、ライセンス管理ファイル１６２１～１６２ｎからエントリ番号を読出せば、ライセンス管理ファイル１６２１～１６２ｎに対応する暗号化コンテンツデータを再生するライセンスがどの領域に格納されているのかが解り、容易にライセンスを取出せることができる。

【０２０５】なお、ライセンス管理ファイル１６２２は、「ライセンス無」を表しているが、これは、たとえば、携帯電話機１００が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当し、暗号化コンテンツデータはメモリ１４１５に存在するが、その暗号化コンテンツデータを再生するライセンスが存在しないことを意味する。

【０２０６】［再生］次に、図２０および図２１を参照してメモリカード１１０に記録されたコンテンツデータの携帯電話機１００（コンテンツ再生デバイスとも言う、以下同じ）における再生動作について説明する。図２０を参照して、再生動作の開始とともに、携帯電話機１００のユーザから操作パネル１１０８を介して再生指示が携帯電話機１００にインプットされる（ステップＳ１０００）。そうすると、コントローラ１１０６は、バスＢＳ３を介して認証データ保持部１５００から認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを読出し、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを出力する（ステップＳ１００２）。

【０２０７】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受理する（ステップＳ１００４）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを、ＫＰａ保持部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ１００６）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ１００８）。復号できなかった場合、ステップＳ１０４８へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、取得したクラス証明書Ｃｐ１がメモリ１４１５から読出した禁止クラスリストデータＣＲＬに含まれるか否かを判断する（ステップＳ１０１０）。この場合、クラス証明書Ｃｐ１にはＩＤが付与されており、コントローラ１４２０は、受理したクラス証明書Ｃｐ１のＩＤが禁止クラスリストデータの中に存在するか否かを判別する。クラス証明書Ｃｐ１が禁止クラスリストデータに含まれると判断されると、ステップＳ１０４８へ移行し、再生動作は終了する。

【０２０８】ステップＳ１０１０において、証明書Ｃｍ１が禁止クラスリストデータＣＲＬに含まれていないと判断されると、メモリカード１１０のセッションキー発

生部１４１８は、再生セッション用のセッションキーＫ—s-2-を発生させる（ステップＳ１０１２）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ１０１４）。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ１０１６）。携帯電話機１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１５０２は、秘密復号鍵Ｋｐ１を復号処理部１５０４へ出力する。

【０２０９】復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ１０１８）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ１０２０）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１０６は、バスＢＳ３およびメモリカードインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ１０２２）。

【０２１０】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して｛Ｋｓ３｝Ｋｓ２を入力する（ステップＳ１０２４）。

【０２１１】図２１を参照して、復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、携帯電話機１００で発生されたセッションキーＫｓ３を受理する（ステップＳ１０２６）。

【０２１２】再生端末のコントローラ１１０６は、メモリカード１１０から事前に取得したライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、メモリカードインタフェース１２００を介してメモリカード１１０へ取得したエントリ番号を出力する（ステップＳ１０２７）。

【０２１３】エントリ番号が入力に応じて、コントローラ１４２０は、ライセンス領域１５１４Ｂの入力されたエントリの再生回数制限ＡＣｍを確認する（ステップＳ１０２８）。ステップＳ１０２８においては、メモリのアクセスに対する制限に関する情報である再生回数制限ＡＣｍを確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数制限に制限がある場合には再生回数制限ＡＣｍのデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ１０３０）。一方、再生回数制限ＡＣｍによって再生回数が制限されていない場合においては、ステップＳ１０３０はスキップされ、再生回数制限ＡＣｍは更新されることなく処理が次のステップ（ステップＳ１０３２）に進行される。

【０２１４】ステップＳ１０２８において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ｃに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生期限ＡＣｐがバスＢＳ４上に出力される（ステップＳ１０３２）。

【０２１５】得られたライセンス鍵Ｋｃと再生期限ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号処理部１４０６に送られる。暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと再生期限ＡＣｐとを暗号化し、｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ４に出力する（ステップＳ１０３４）。

【０２１６】バスＢＳ４に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して携帯電話機１００に送出される。

【０２１７】携帯電話機１００においては、メモリカードインタフェース１２００を介してバスＢＳ３に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生期限ＡＣｐを受理する（ステップＳ１０３６）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生期限ＡＣｐをバスＢＳ３に出力する。

【０２１８】コントローラ１１０６は、バスＢＳ３を介して、再生期限ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ１０４０）。

【０２１９】ステップＳ１０４０においては、再生期限ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

【０２２０】ステップＳ１０４０において再生可能と判断された場合、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ４、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する（ステップＳ１０４２）。

【０２２１】携帯電話機１００のコントローラ１１０６

は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１６へ与える。

【０２２２】そして、復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ１０４４）。

【０２２３】そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホーン１３０へ出力されて再生される（ステップＳ１０４６）。これによって再生動作が終了する。

【０２２４】上記においては、メモリカード１１０に記録された暗号化コンテンツデータを携帯電話機１００によって再生する場合について説明したが、パーソナルコンピュータ５０のコンテンツ再生デバイス１５５０は、ＨＤＤ５３０に記憶された暗号化コンテンツデータをライセンス管理デバイス５２０に格納されたライセンスによって再生することができるが、その時の動作は図２０および図２１に示すフローチャートに従って行われる。

【０２２５】上記においては、ＣＤ－ＲＯＭ６０から暗号化コンテンツデータを取得したパーソナルコンピュータ５０は、配信サーバ１０から暗号化コンテンツデータを再生するライセンスを受信し、暗号化コンテンツデータとライセンスとを携帯電話機１００に装着されたメモリカード１１０に移動する移動セッションについて説明した。したがって、本発明においては、図２２に示すデータ配信システムも可能である。

【０２２６】すなわち、パーソナルコンピュータ５０がＣＤ－ＲＯＭ６０から暗号化コンテンツデータとサーバ情報ファイルとを取得し、その取得したサーバ情報ファイルに基づいて配信サーバ１０に接続し、配信サーバ１０からライセンスを受信する点は、図１に示すデータ配信システムと同じである。図２２においては、パーソナルコンピュータ５０は、取得した暗号化コンテンツデータおよびライセンスをＵＳＢケーブル７０，７１を介して端末装置１２０，１２１へ移動する。

【０２２７】端末装置１２０，１２１は、データを配信サーバ１０との間で送受信する通信機能を有しない端末装置であり、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０と同じ構成のデバイスが内蔵されている。そして、端末装置１２０，１２１は、パーソナルコンピュータ５０から受信したライセンスを内蔵したデバイスに格納する。また、端末装置１２０，１２１は、暗号化コンテンツデータをハードディスク等に格納して管理する。さらに、端末装置１２０，１２１は、上述したコンテンツ再生デバイス１５５０を内蔵しており、パーソナルコンピュータ５０から受信した暗号化コンテンツデータを再生することも可能である。

【０２２８】図２２に示すデータ配信システムによれば、配信サーバ１０との通信機能を持たず、かつ、ＣＤ－ＲＯＭ６０から暗号化コンテンツデータを取得する機能も持たない端末装置であっても、ＣＤ－ＲＯＭ６０に記録された音楽データをライセンスとともに取得することができる。

【０２２９】本発明の実施の形態によれば、パーソナルコンピュータは音楽ＣＤから暗号化コンテンツデータを取得する際、サーバへのアクセス手段やアクセス先を含むサーバ情報ファイルも取得するので、暗号化コンテンツデータの取得と同時に暗号化コンテンツデータを再生するライセンスを配信サーバから受信できる。

【０２３０】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　本発明の実施の形態におけるデータ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図５】　図１に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図である。

【図６】　図１に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図７】　図１に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図８】　図５に示すパーソナルコンピュータに内蔵されたライセンス管理デバイスの構成を示す概略ブロック図である。

【図９】　図１に示すデータ配信システムにおけるライセンスの配信動作を説明するための第１のフローチャートである。

【図１０】　図１に示すデータ配信システムにおけるライセンスの配信動作を説明するための第２のフローチャートである。

【図１１】　図１に示すデータ配信システムにおけるライセンスの配信動作を説明するための第３のフローチャートである。

【図１２】　図１に示すデータ配信システムにおけるラ

イセンスの配信動作を説明するための第４のフローチャートである。

【図１３】　図１に示すデータ配信システムにおけるライセンスの配信動作を説明するための第５のフローチャートである。

【図１４】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第１のフローチャートである。

【図１５】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第２のフローチャートである。

【図１６】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第３のフローチャートである。

【図１７】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第４のフローチャートである。

【図１８】　パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

【図１９】　メモリカードにおける再生リストファイルの構成を示す図である。

【図２０】　携帯電話機における再生動作を説明するための第１のフローチャートである。

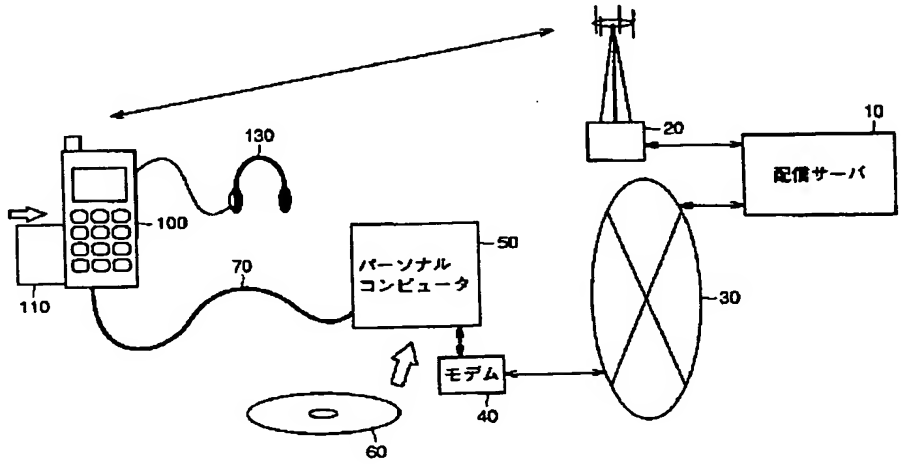
【図２１】　携帯電話機における再生動作を説明するための第２のフローチャートである。

【図２２】　本発明の実施の形態における他のデータ配信システムを概念的に説明する概略図である。

【符号の説明】

１０　配信サーバ、２０　配信キャリア、３０　インターネット網、４０　モデム、５０，８０　パーソナルコンピュータ、６０　ＣＤ、７０，７１　ＵＳＢケーブル、１００　携帯電話機、１１０　メモリカード、１２０，１２１　端末装置、１３０　ヘッドホーン、１５０　コンテンツリストファイル、１６０　再生リストファイル、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６，５２０４，５２０８，５２１２，５２２２　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６，５２０６，５２１０，５２１７，５４０５　暗号処理部、３５０　通信装置、５１０，１１０６，１４２０，５２２０　コントローラ、５１１，８１１　ライセンス管理モジュール、５２０，８２０　ライセンス管理デバイス、５３０　ハードディスク、５４０　ＣＤ－ＲＯＭドライブ、５５０，１１１２　ＵＳＢインタフェース、５６０　キーボード、５７０　ディスプレイ、５８０，１１１４，１４２６，１５３０，５２２６　端子、１１０８　操作パネル、１１１０　表示パネル、１２００　メモリカードインタフェース、１４００，１５００，５２００　認証データ保持部、１４０２，５２０２　Ｋｍｃ保持部、１４１４，５２１４　ＫＰａ保持部、１４１５，５２１５　メモリ、１４１５Ａ，５２１５Ａ　ＣＲＬ領域、１４１５Ｂ　再生リスト領域、１４１５Ｃ，５２１５Ｂ　ライセンス領域、１４１５Ｄ　データ領域、１４１６，５２１６ＫＰｍｃ保持部、１４１８，５２１８　セッションキー発生部、１４２１，５２２１　Ｋｍ保持部、１４２４，５２２４　インタフェース、１４４２，１４４６切換スイッチ、１５０２　Ｋｐ１保持部、１５１８　音楽再生部、１５１９ＤＡ変換器、１５２１～１５２ｎ，１６２１～１６２ｎ　ライセンス管理ファイル、１５３１～１５３ｎ，１６１１～１６１２ｎ　コンテンツファイル、１５５０　コンテンツ再生デバイス。

【図１】



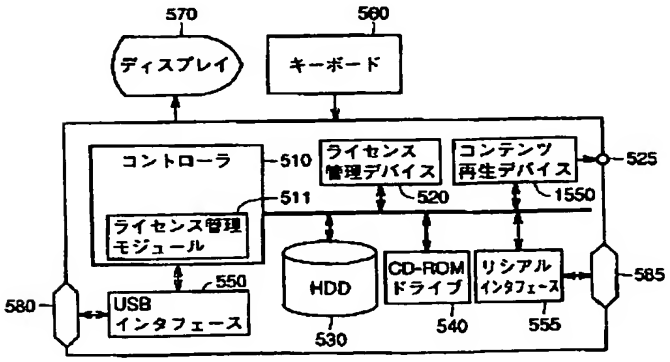
【図２】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス鍵 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID＋コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc＋ACm＋ACp＋ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止認証データのリスト CRLの更新日(CRLdate)を含む

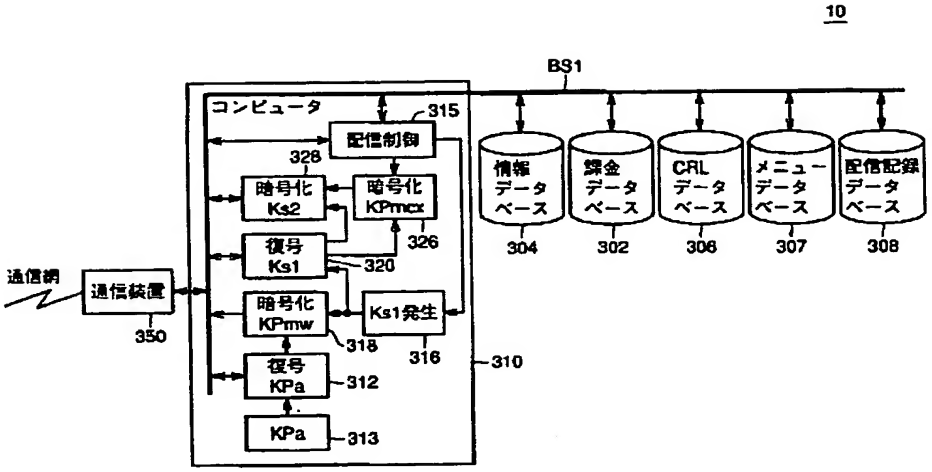
【図３】

	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 メモリカードおよびコンテンツ管理モジュールと同一
	Ks1	共通鍵	セッション固有	メモリカードライセンス管理デバイス、ライセンス管理モジュールへのライセンス配信ごとに発生
メモリカード ライセンス管理デバイス（ハードタンパ） ライセンス管理モジュール（ソフトタンパ）	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 配信サーバと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。認証機能を有する。 {KPmw//Cmw}KPaの形式で出荷時に記録。 ※メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスwごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 {KPpy//Cpy}KPaの形式で出荷時に記録。 ※コンテンツ再生デバイスのクラスyごとに異なる。

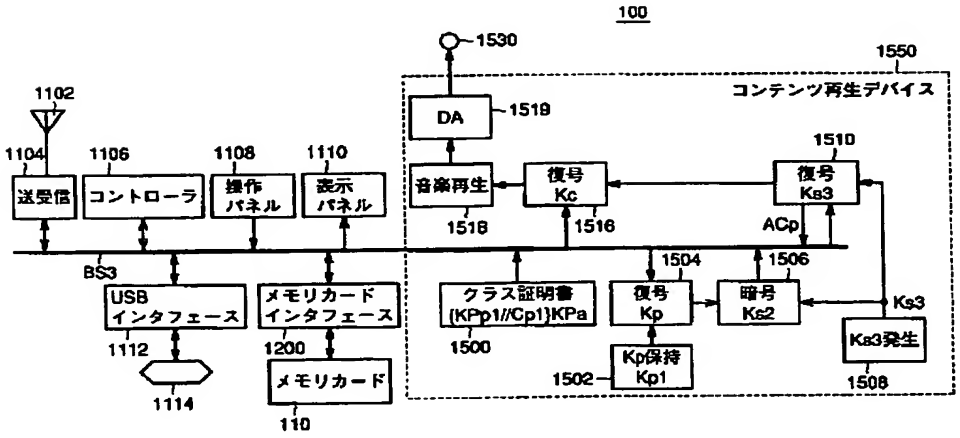
【図５】



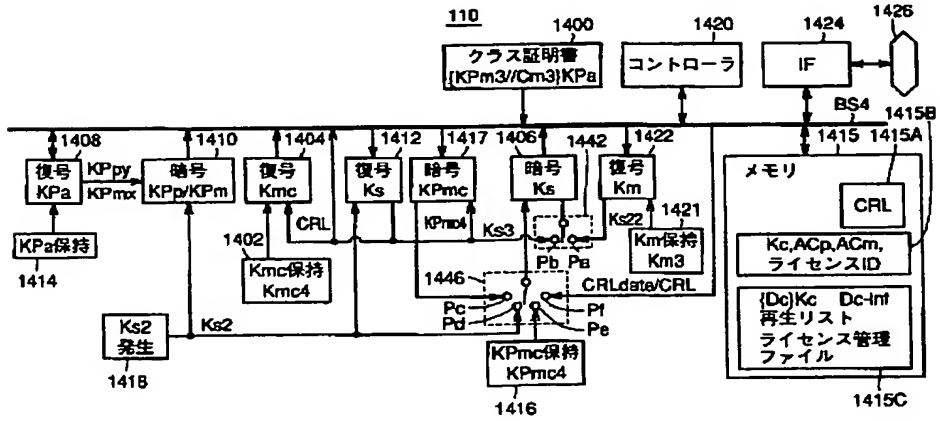
【図４】


10
BS1
コンピュータ
315
配信制御
328
暗号化 Ks2
暗号化 KPmcx
326
復号 Ks1
320
暗号化 KPmw
318
Ks1発生
316
310
復号 KPa
312
KPa
313
通信網
通信装置
350
情報データベース
304
課金データベース
302
CRLデータベース
306
メニューデータベース
307
配信記録データベース
308

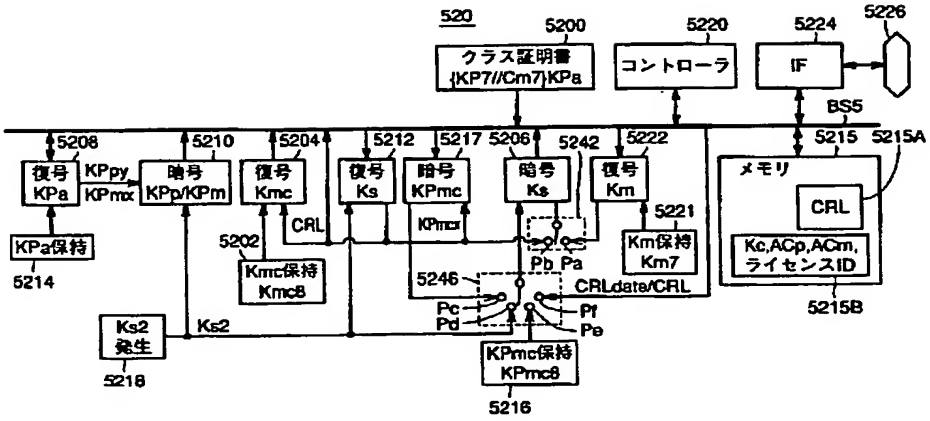
【図６】


100
1530
1550
コンテンツ再生デバイス
1102
1104
1106
1108
1110
送受信
コントローラ
操作パネル
表示パネル
DA
1519
音楽再生
1518
復号 Kc
1516
1510
復号 Ks3
ACp
1504
1506
BS3
USBインタフェース
1112
1114
メモリカードインタフェース
1200
メモリカード
110
クラス証明書 {KPp1//Cp1}KPa
1500
復号 Kp
暗号 Ks2
Ks3
Ks3発生
1508
Kp保持 Kp1
1502

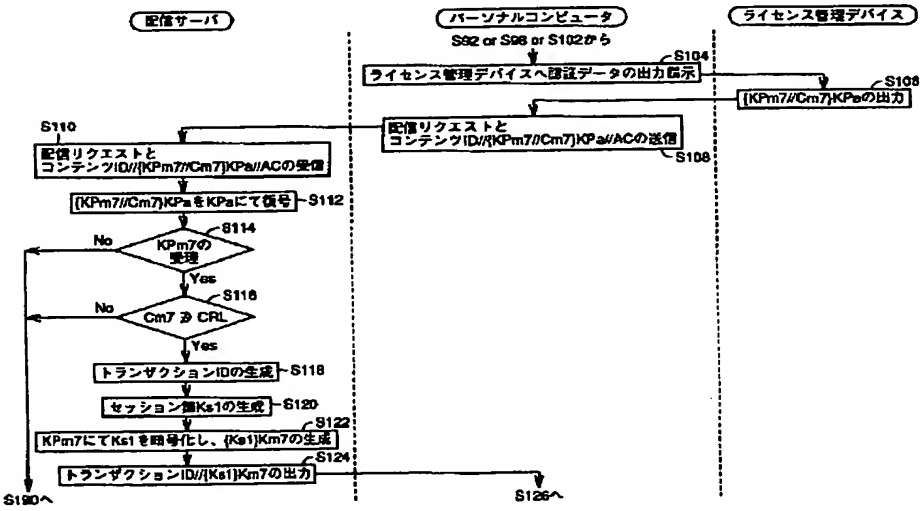
【図７】


110
1400
クラス証明書 {KPm3//Cm3}KPa
1420
コントローラ
1424
IF
1426
BS4
1415B
1408
1410
1404
1412
1417
1406
1442
1422
1415
1415A
復号 KPa
KPpy
KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
メモリ
CRL
KPa保持
1414
1402
Kmc保持 Kmc4
CRL
KPmc4
Ks3
Ks22
1421
Km保持 Km3
Pb Pa
1446
CRLdate/CRL
Kc,ACp,ACm, ライセンスID
Pc
Pd
Pf
Pe
{Dc}Kc Dc-Inf
再生リスト
ライセンス管理ファイル
Ks2
Ks2発生
1418
KPmc保持 KPmc4
1416
1415C

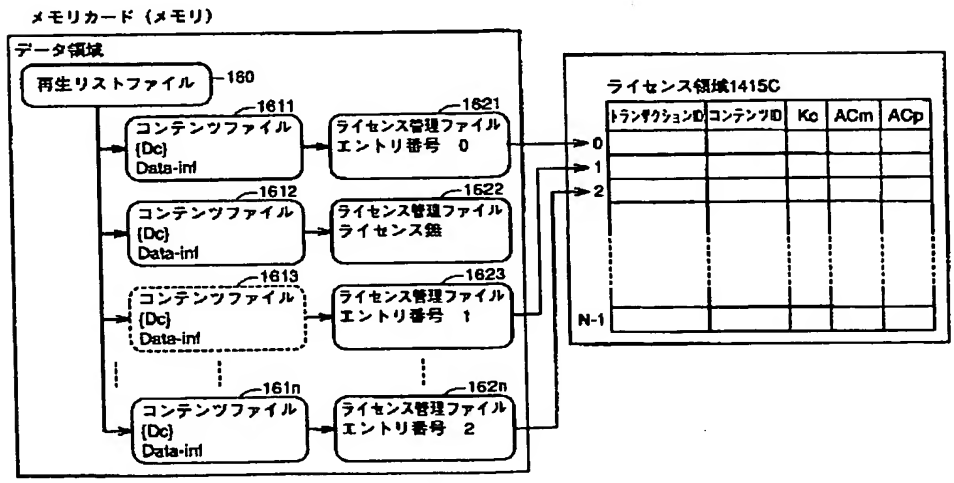
【図８】


520
5200
クラス証明書
{KP7//Cm7}KPs
5220
コントローラ
5224
IF
5226
BS5
5208
復号
KPa
KPpy
KPmx
5210
暗号
KPp/KPm
5204
復号
Kmc
5212
復号
Ks
5217
暗号
KPmc
5206
暗号
Ks
5242
5222
復号
Km
5215
メモリ
5215A
CRL
Kc,ACp,ACm,
ライセンスID
5215B
5221
Km保持
Km7
KPa保持
5214
5202
Kmc保持
Kmc8
CRL
KPmcr
Pb Pa
5246
CRLdate/CRL
Pc
Pd
Pf
Pe
Ks2
発生
5218
Ks2
KPmc保持
KPmc8
5216

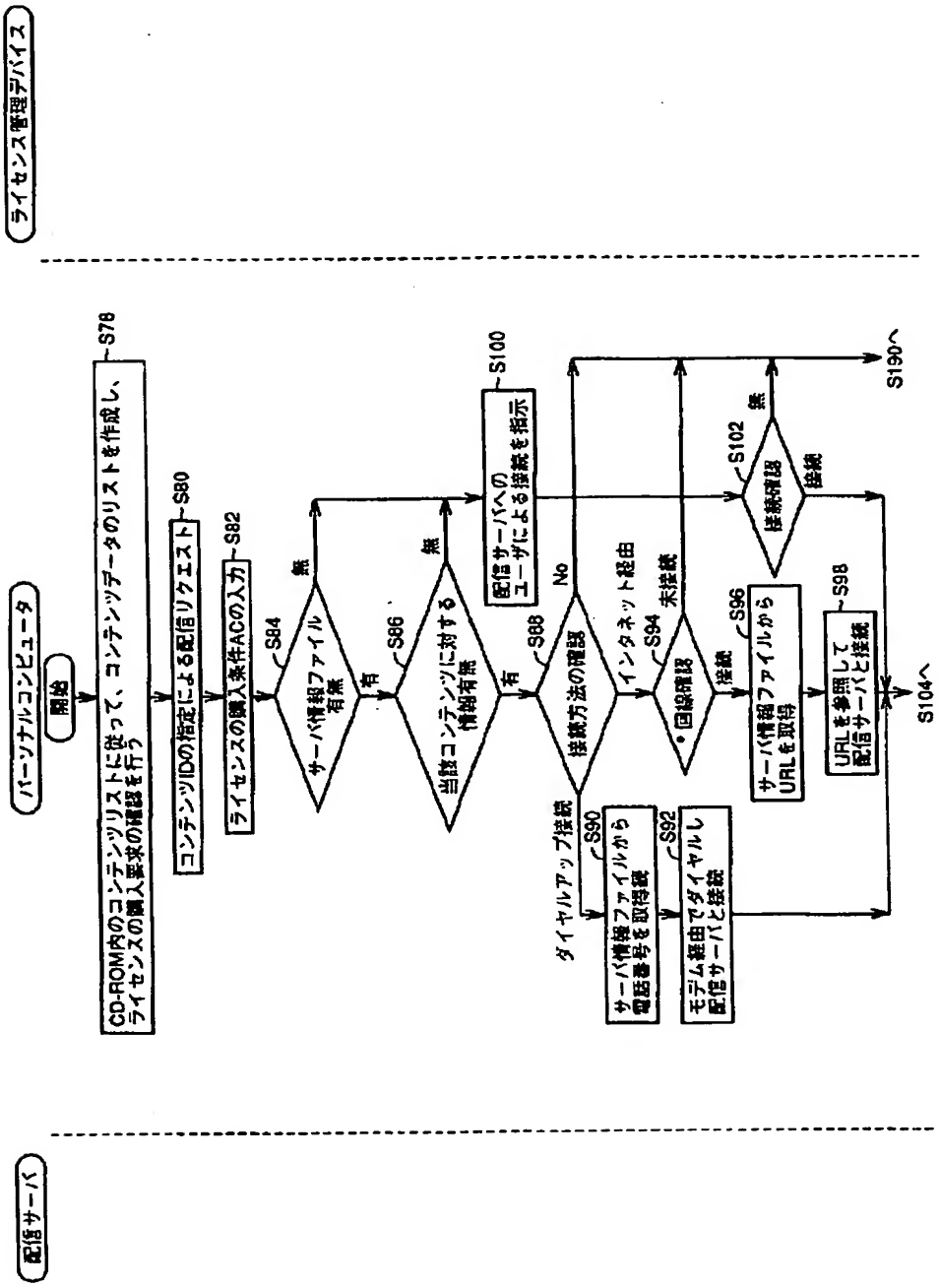
【図１０】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
S92 or S98 or S102から
S104
ライセンス管理デバイスへ認証データの出力指示
S106
{KPm7//Cm7}KPsの出力
S110
配信リクエストと
コンテンツID//{KPm7//Cm7}KPa//ACの受信
配信リクエストと
コンテンツID//{KPm7//Cm7}KPa//ACの送信
S108
{KPm7//Cm7}KPsをKPaにて復号
S112
S114
KPm7の
受理
No
Yes
S116
Cm7 ∋ CRL
No
Yes
トランザクションIDの生成
S118
セッション鍵Ks1の生成
S120
S122
KPm7にてKs1を暗号化し、{Ks1}Km7の生成
S124
トランザクションID//{Ks1}Km7の出力
S130へ
S126へ

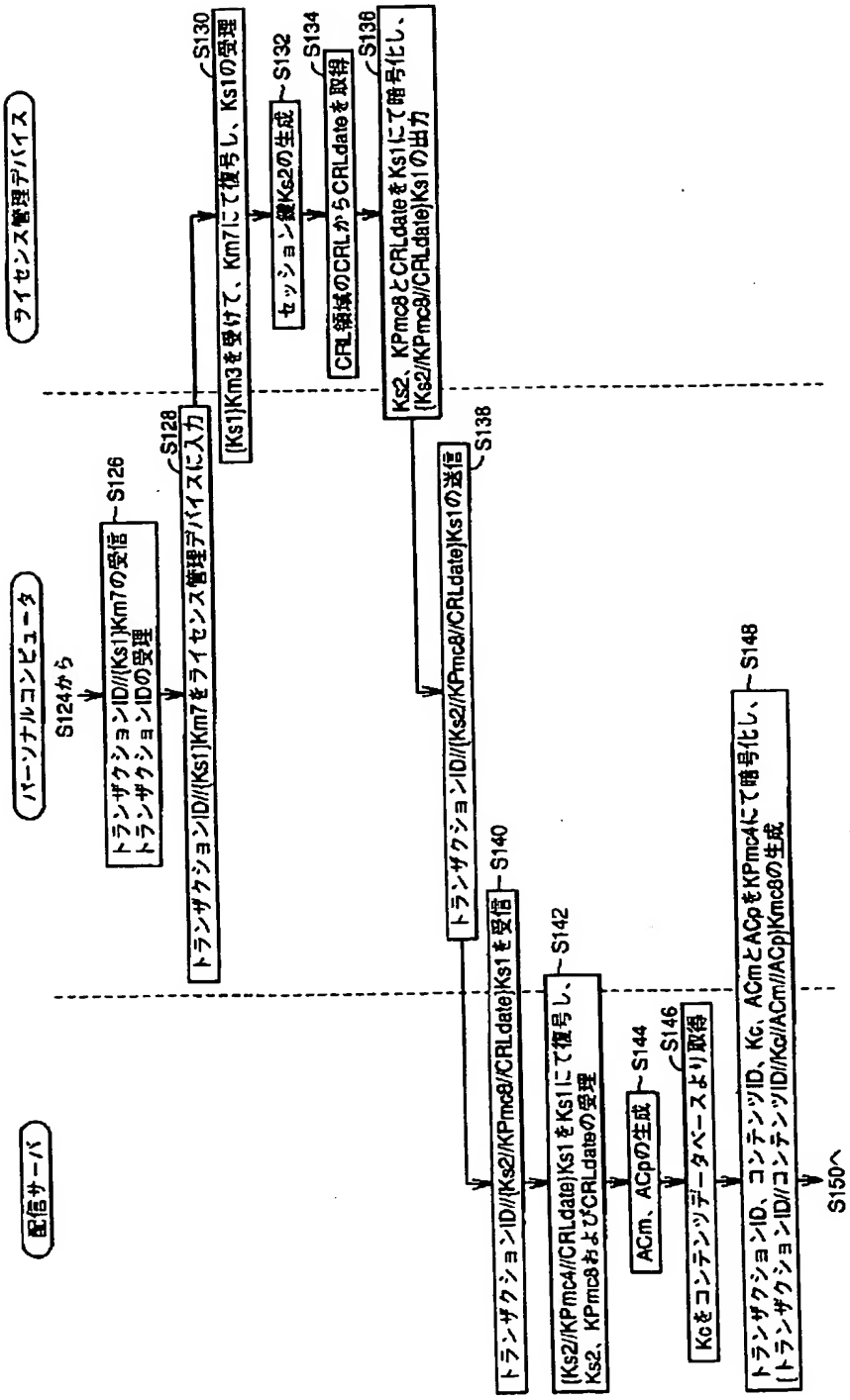
【図１９】


メモリカード（メモリ）
データ領域
再生リストファイル
160
1611
コンテンツファイル
{Dc}
Data-inf
1621
ライセンス管理ファイル
エントリ番号　0
1612
コンテンツファイル
{Dc}
Data-inf
1622
ライセンス管理ファイル
ライセンス無
1613
コンテンツファイル
{Dc}
Data-inf
1623
ライセンス管理ファイル
エントリ番号　1
161n
コンテンツファイル
{Dc}
Data-inf
162n
ライセンス管理ファイル
エントリ番号　2
ライセンス領域1415C
トランザクションID
コンテンツID
Kc
ACm
ACp
0
1
2
N-1

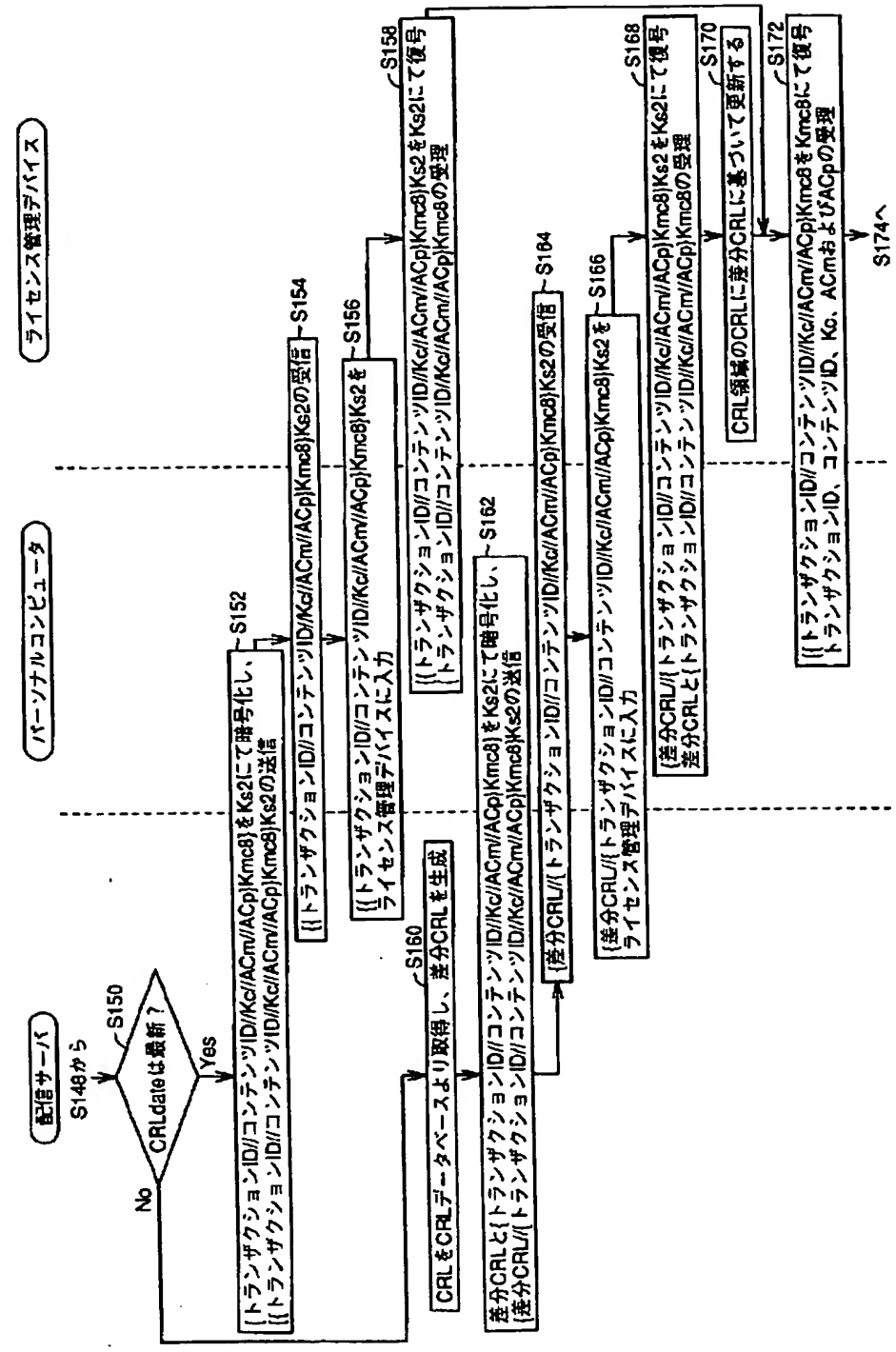
【図９】


ライセンス管理デバイス
パーソナルコンピュータ
開始
CD-ROM内のコンテンツリストに従って、コンテンツデータのリストを作成し、ライセンスの購入要求の確認を行う
S78
コンテンツIDの指定による配信リクエスト
S80
ライセンスの購入条件ACの入力
S82
S84
サーバ情報ファイル有無
無
有
S86
当該コンテンツに対する情報有無
無
有
S88
接続方法の確認
No
ダイヤルアップ接続
S90
サーバ情報ファイルから電話番号を取得
S92
モデム経由でダイヤルし配信サーバと接続
インターネット経由
S94
回線確認
未接続
接続
S96
サーバ情報ファイルからURLを取得
S98
URLを参照して配信サーバと接続
S100
配信サーバへのユーザによる接続を指示
S102
接続確認
無
接続
S190へ
S104へ
配信サーバ

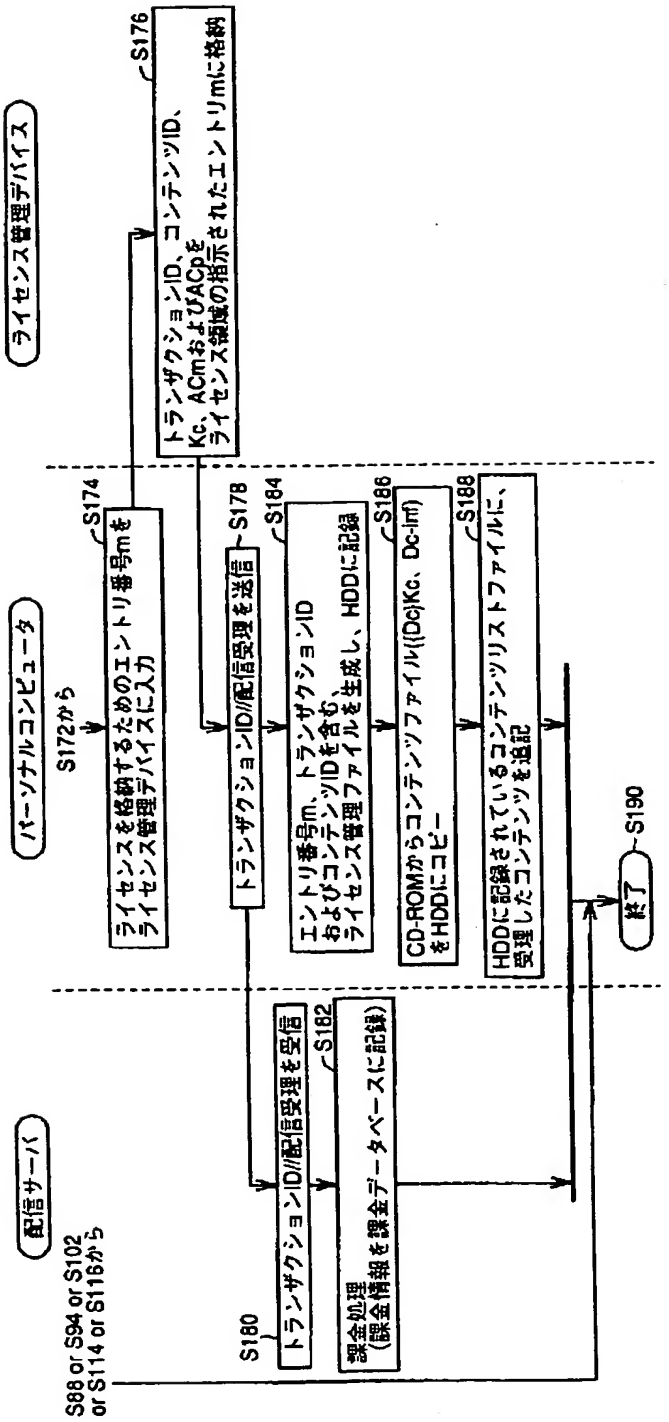
【図１１】


ライセンス管理デバイス
パーソナルコンピュータ
配信サーバ
S124から
トランザクションID//[(Ks1)Km7の受信
トランザクションIDの受理
S126
トランザクションID//[(Ks1)Km7をライセンス管理デバイスに入力
S128
[(Ks1)Km3を受けて、Km7にて復号し、Ks1の受理
S130
セッション鍵Ks2の生成
S132
CRL領域のCRLからCRLdateを取得
S134
Ks2、KPmc8とCRLdateをKs1にて暗号化し、
[(Ks2//KPmc8//CRLdate)Ks1の出力
S136
トランザクションID//[(Ks2//KPmc8//CRLdate)Ks1の送信
S138
トランザクションID//[(Ks2//KPmc8//CRLdate)Ks1を受信
S140
[(Ks2//KPmc4//CRLdate)Ks1をKs1にて復号し、
Ks2、KPmc8およびCRLdateの受理
S142
ACm、ACpの生成
S144
Koをコンテンツデータベースより取得
S146
トランザクションID、コンテンツID、Kc、ACmとACpをKPmc4にて暗号化し、
[(トランザクションID//コンテンツID//Kc//ACm//ACp)Kmc8の生成
S148
S150へ

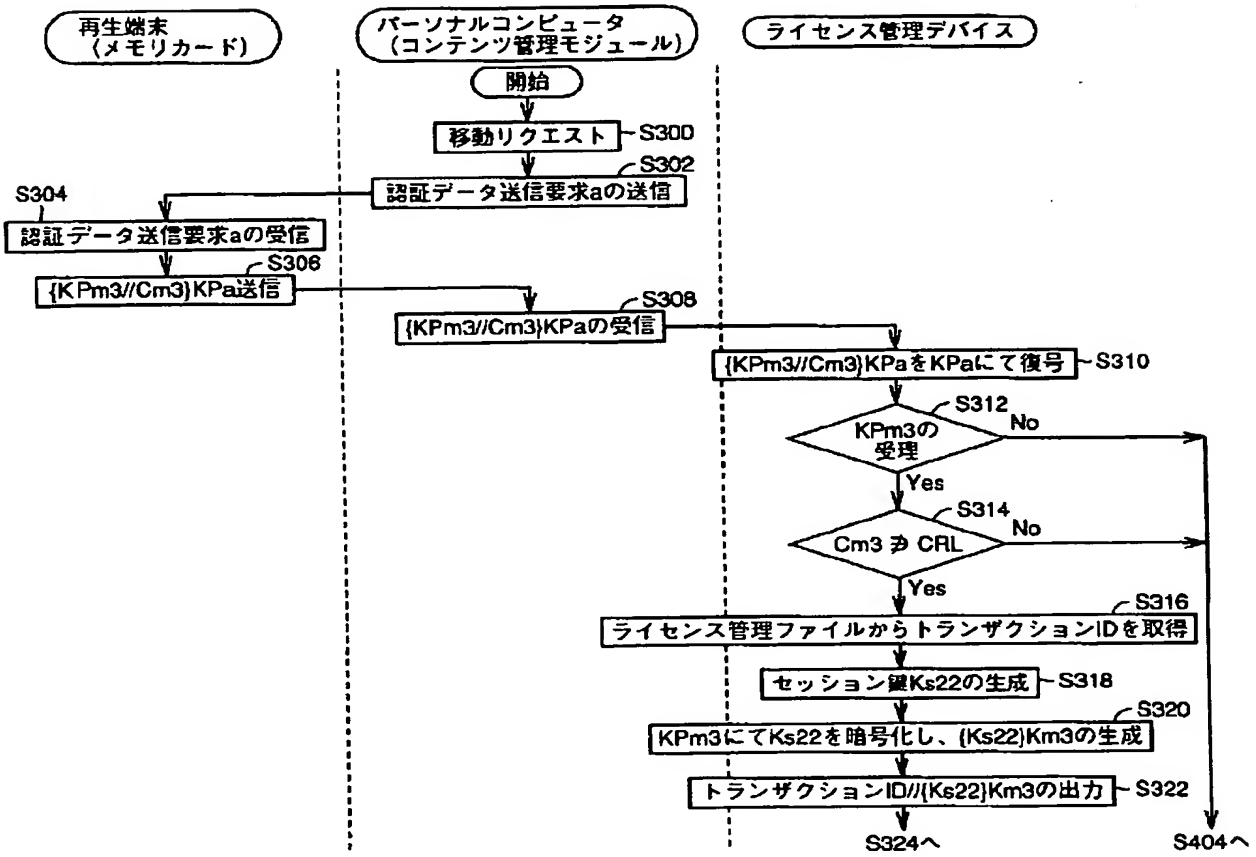
【図１２】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
S148から
S150
CRLdateは最新？
No
Yes
S152
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の送信
S154
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の受信
S156
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を
ライセンス管理デバイスに入力
S158
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をKs2にて復号
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の受理
S160
CRLをCRLデータベースより取得し、差分CRLを生成
S162
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}をKs2にて暗号化し、
差分CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の送信
S164
{差分CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の受信
S166
{差分CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を
ライセンス管理デバイスに入力
S168
{差分CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をKs2にて復号
差分CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の受理
S170
CRL領域のCRLに差分CRLに基づいて更新する
S172
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}をKmc8にて復号
{{トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S174へ

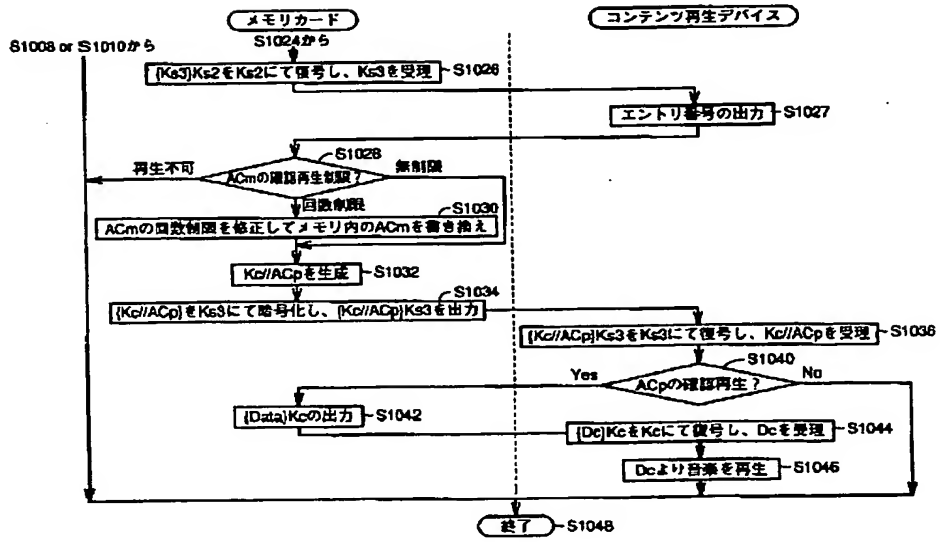
【図１３】


ライセンス管理デバイス
パーソナルコンピュータ
配信サーバ
S88 or S94 or S102
or S114 or S116から
S172から
ライセンスを格納するためのエントリ番号mを
ライセンス管理デバイスに入力
S174
トランザクションID//配信受理を送信
S178
トランザクションID//配信受理を受信
S180
課金処理
(課金情報を課金データベースに記録)
S182
トランザクションID、コンテンツID、
Kc、ACmおよびACpを
ライセンス領域の指示されたエントリmに格納
S176
エントリ番号m、トランザクションID
およびコンテンツIDを含む、
ライセンス管理ファイルを生成し、HDDに記録
S184
CD-ROMからコンテンツファイル({Dc}Kc、Dc-inf)
をHDDにコピー
S186
HDDに記録されているコンテンツリストファイルに、
受理したコンテンツを追記
S188
終了
S190

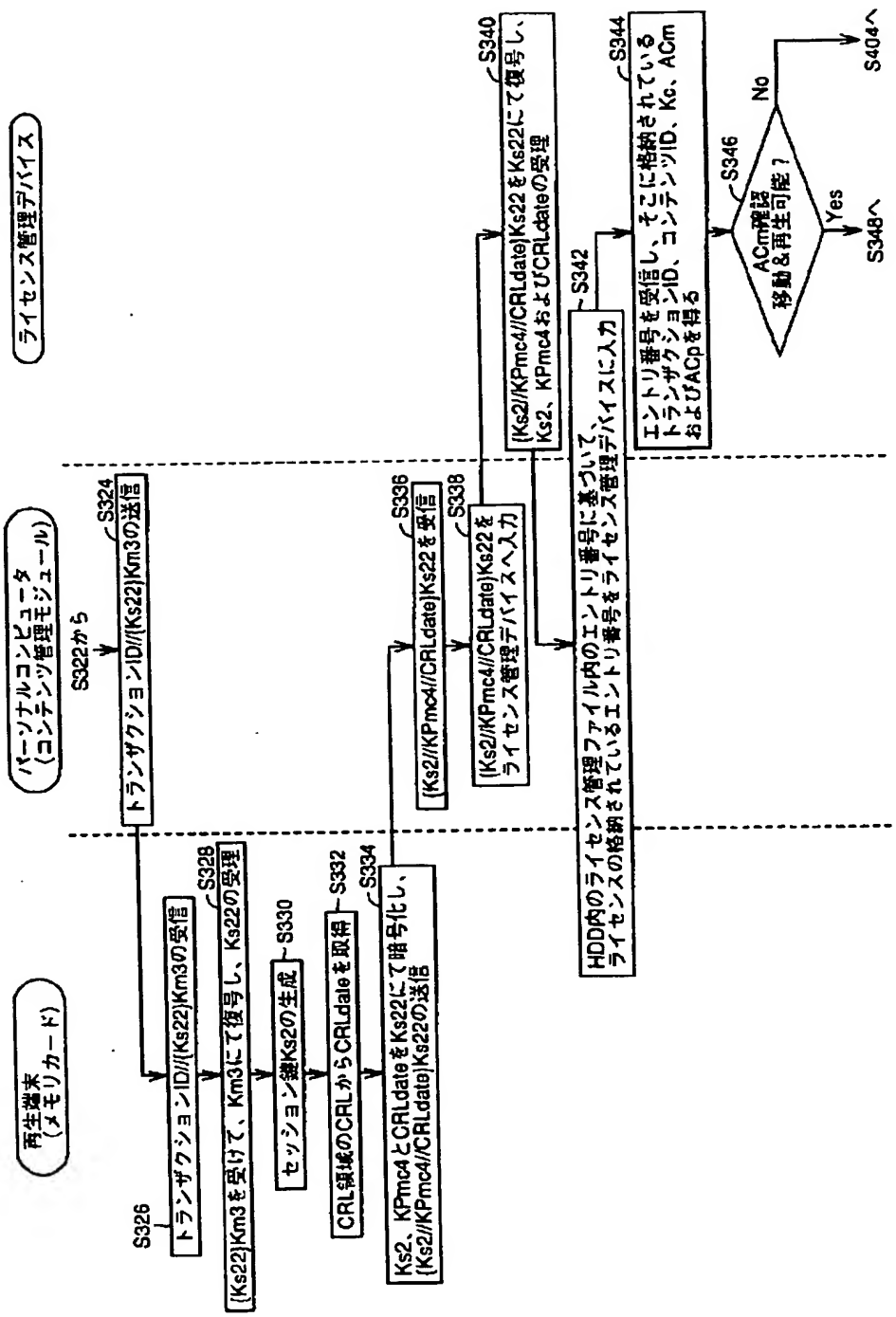
【図１４】


再生端末
(メモリカード)
パーソナルコンピュータ
(コンテンツ管理モジュール)
ライセンス管理デバイス
開始
移動リクエスト
S300
S302
認証データ送信要求aの送信
S304
認証データ送信要求aの受信
S306
{KPm3//Cm3}KPa送信
S308
{KPm3//Cm3}KPaの受信
{KPm3//Cm3}KPaをKPaにて復号
S310
S312
KPm3の受理
No
Yes
S314
Cm3 ≠ CRL
No
Yes
S316
ライセンス管理ファイルからトランザクションIDを取得
セッション鍵Ks22の生成
S318
S320
KPm3にてKs22を暗号化し、{Ks22}Km3の生成
トランザクションID//{Ks22}Km3の出力
S322
S324へ
S404へ

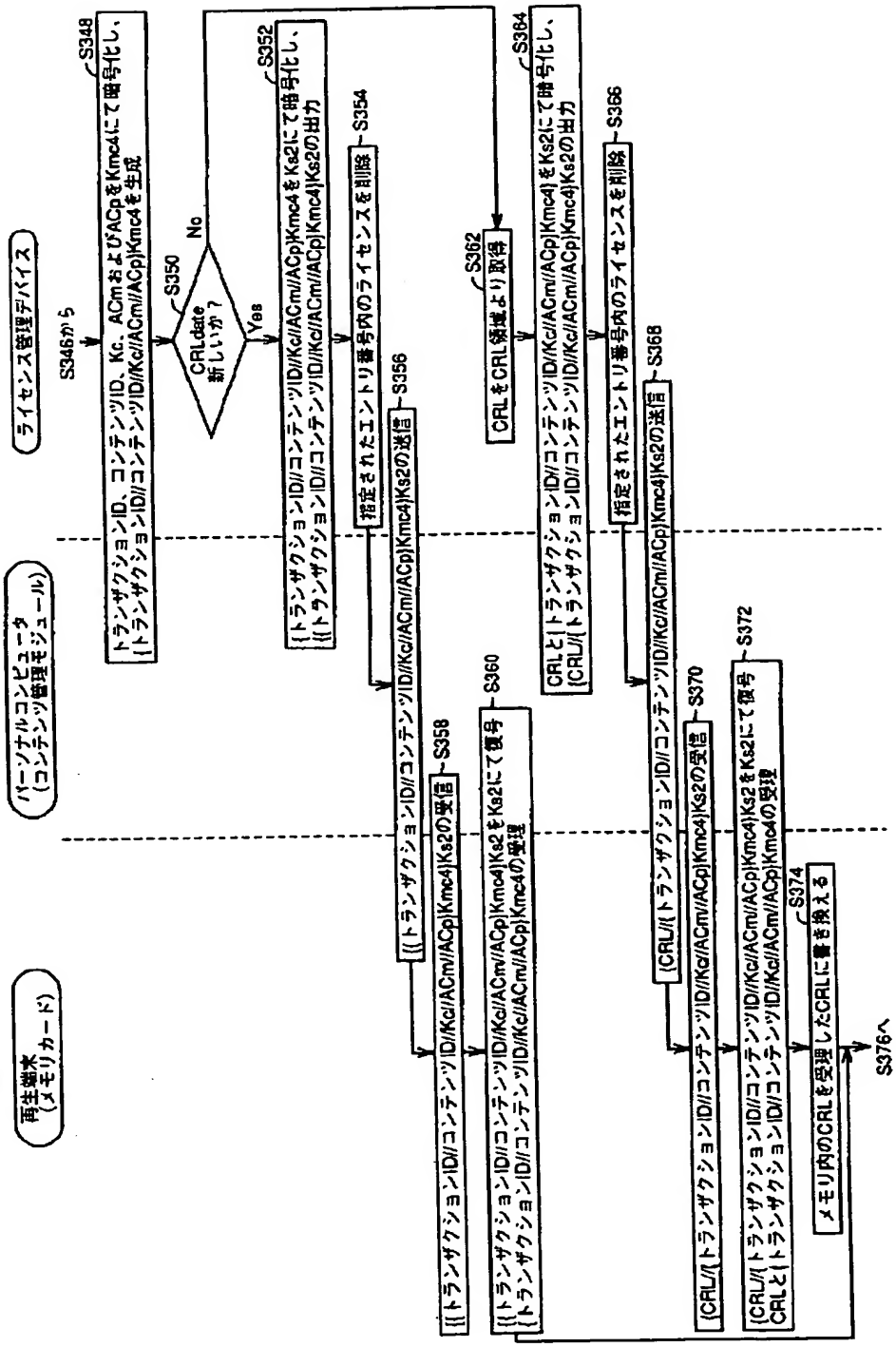
【図２１】


メモリカード
コンテンツ再生デバイス
S1008 or S1010から
S1024から
{Ks3}Ks2をKs2にて復号し、Ks3を受理
S1026
エントリ番号の出力
S1027
S1028
ACmの繰返再生制限？
再生不可
無制限
回数制限
S1030
ACmの回数制限を修正してメモリ内のACmを書き換え
Kc//ACpを生成
S1032
{Kc//ACp}をKs3にて暗号化し、{Kc//ACp}Ks3を出力
S1034
{Kc//ACp}Ks3をKs3にて復号し、Kc//ACpを受理
S1036
S1040
ACpの繰返再生？
Yes
No
{Data}Kcの出力
S1042
{Dc}KcをKcにて復号し、Dcを受理
S1044
Dcより音楽を再生
S1046
終了
S1048

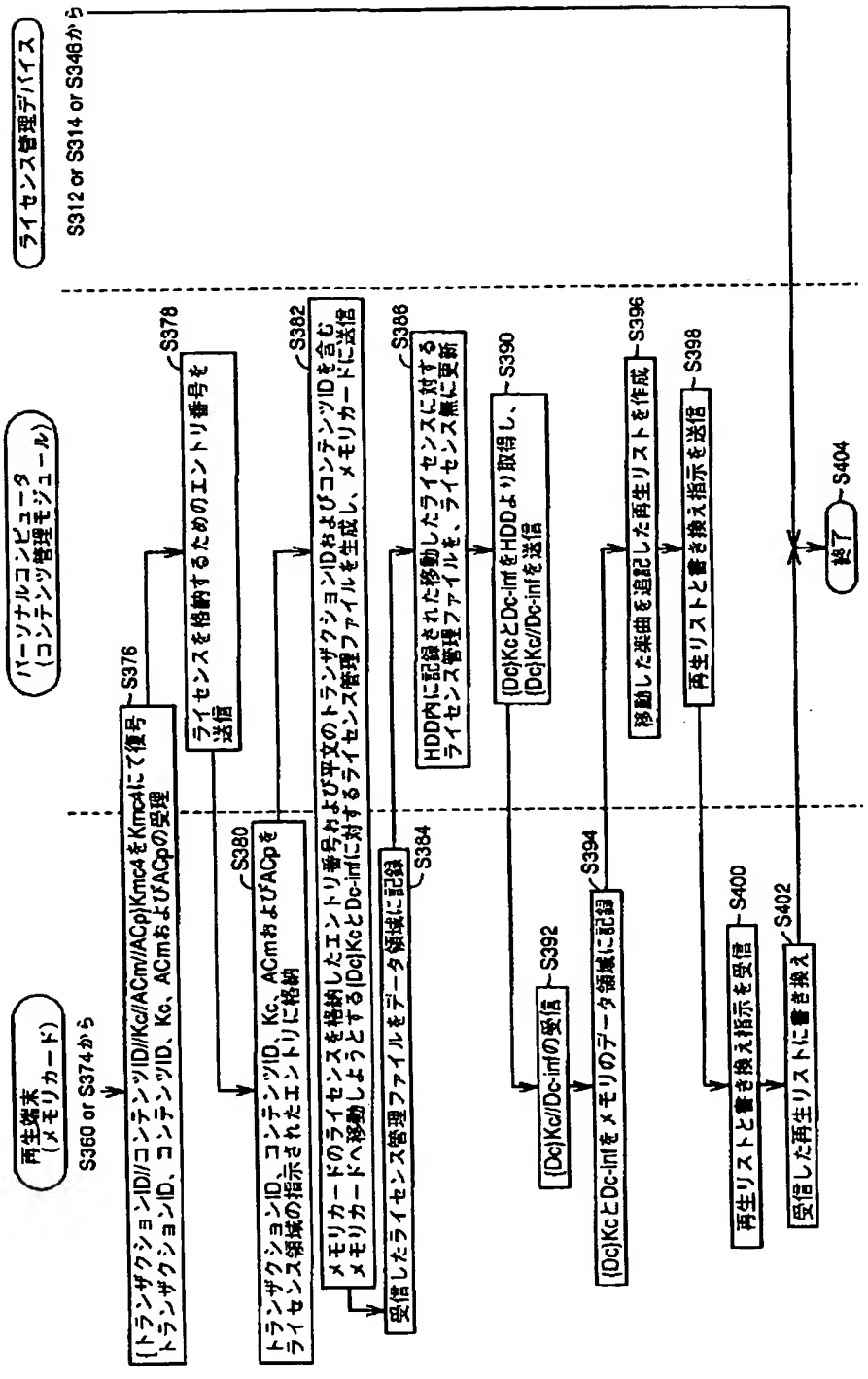
【図１５】


再生端末
(メモリカード)
パーソナルコンピュータ
(コンテンツ管理モジュール)
ライセンス管理デバイス
S322から
S324
トランザクションID//{Ks22}Km3の送信
S326
トランザクションID//{Ks22}Km3の受信
S328
{Ks22}Km3を受けて、Km3にて復号し、Ks22の受理
S330
セッション鍵Ks2の生成
S332
CRL領域のCRLからCRLdateを取得
S334
Ks2、KPmc4とCRLdateをKs22にて暗号化し、
{Ks2//KPmc4//CRLdate}Ks22の送信
S336
{Ks2//KPmc4//CRLdate}Ks22を受信
S338
{Ks2//KPmc4//CRLdate}Ks22を
ライセンス管理デバイスへ入力
S340
{Ks2//KPmc4//CRLdate}Ks22をKs22にて復号し、
Ks2、KPmc4およびCRLdateの受理
S342
HDD内のライセンス管理ファイル内のエントリ番号に基づいて、
ライセンスの格納されているエントリ番号をライセンス管理デバイスに入力
S344
エントリ番号を受信し、そこに格納されている
トランザクションID、コンテンツID、Kc、ACm
およびACpを得る
S346
ACm確認
移動&再生可能？
No
S404へ
Yes
S348へ

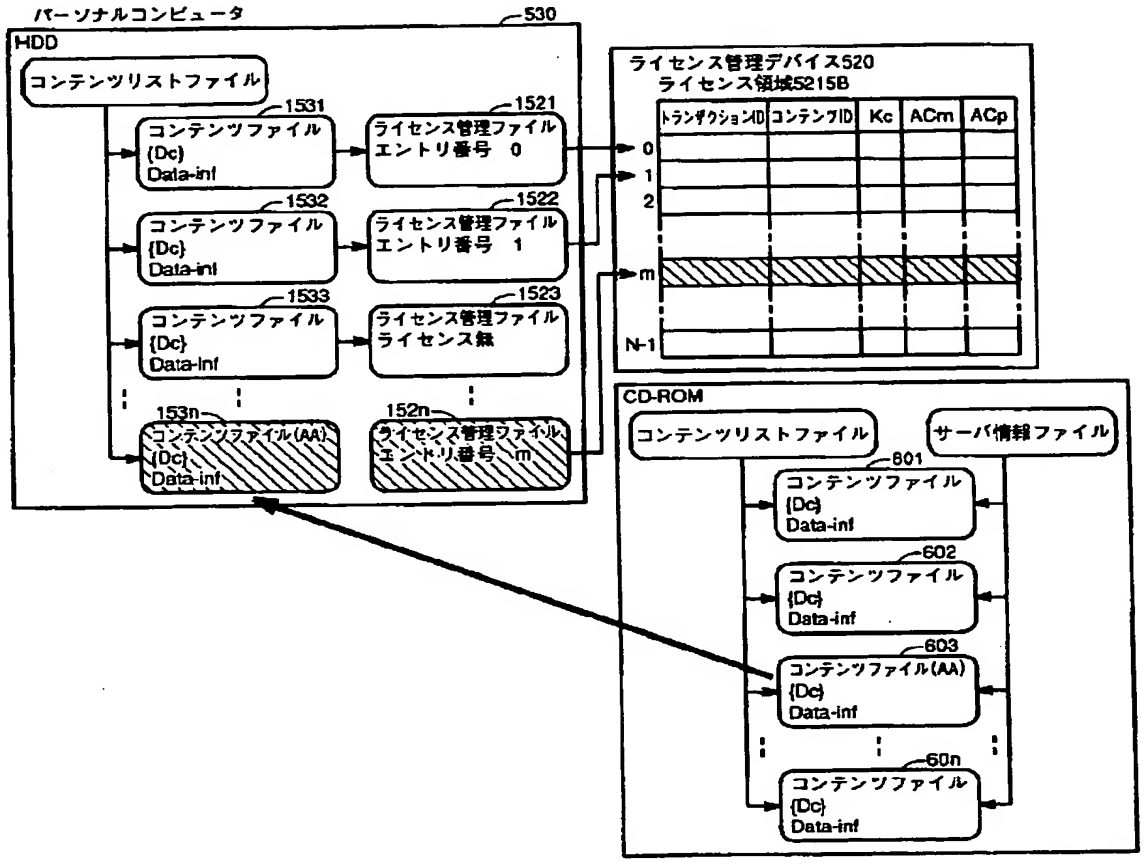
【図１６】


再生端末
(メモリカード)
パーソナルコンピュータ
(コンテンツ管理モジュール)
ライセンス管理デバイス
S346から
S348
トランザクションID、コンテンツID、Kc、ACmおよびACpをKmc4にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}を生成
S350
CRL date
新しいか？
No
Yes
S352
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4をKs2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の出力
S354
指定されたエントリ番号内のライセンスを削除
S356
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の送信
S358
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の受信
S360
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2にて復号
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}の受理
S362
CRLをCRL領域より取得
S364
CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}をKs2にて暗号化し、
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の出力
S366
指定されたエントリ番号内のライセンスを削除
S368
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の送信
S370
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の受信
S372
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2にて復号
CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}の受理
S374
メモリ内のCRLを受理したCRLに書き換える
S376へ

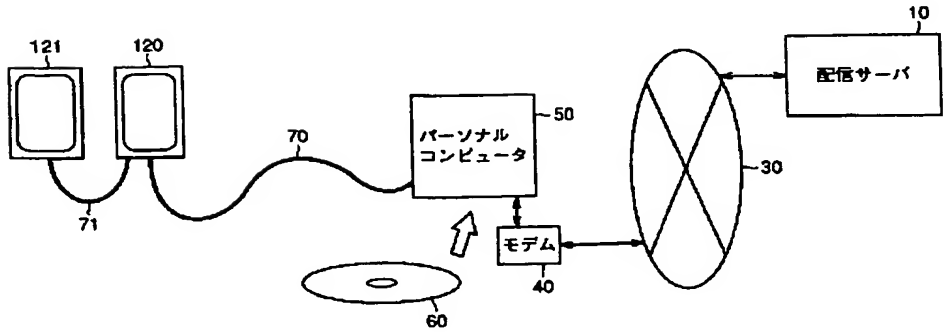
【図１７】


再生端末
(メモリカード)
S360 or S374から
パーソナルコンピュータ
(コンテンツ管理モジュール)
ライセンス管理デバイス
S312 or S314 or S346から
[トランザクションID//コンテンツID//Kc//ACm//ACp]Kmc4をKmc4にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S376
ライセンスを格納するためのエントリ番号を送信
S378
トランザクションID、コンテンツID、Kc、ACmおよびACpをライセンス領域の指示されたエントリに格納
S380
メモリカードのライセンスを格納したエントリ番号および平文のトランザクションIDおよびコンテンツIDを含むメモリカードへ移動しようとする[Dc]KcとDc-infに対するライセンス管理ファイルを生成し、メモリカードに送信
S382
受信したライセンス管理ファイルをデータ領域に記録
S384
HDD内に記録されたライセンスに対するライセンス管理ファイルを、ライセンス無に更新
S386
[Dc]KcとDc-infをHDDより取得し、
[Dc]Kc//Dc-infを送信
S390
[Dc]Kc//Dc-infの受信
S392
[Dc]KcとDc-infをメモリのデータ領域に記録
S394
移動した楽曲を追記した再生リストを作成
S396
再生リストと書き換え指示を送信
S398
再生リストと書き換え指示を受信
S400
受信した再生リストに書き換え
S402
終了
S404

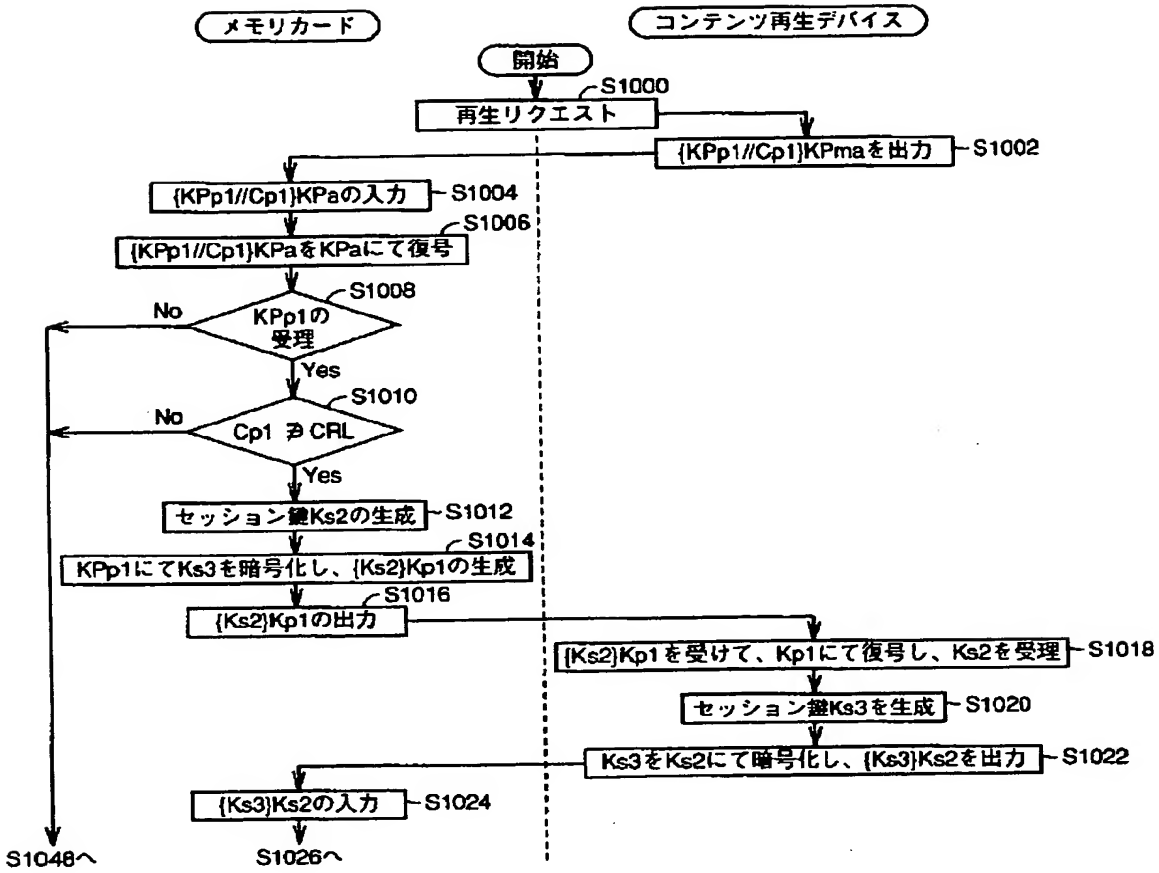
【図１８】


パーソナルコンピュータ
530
HDD
コンテンツリストファイル
1531
コンテンツファイル
{Dc}
Data-inf
1521
ライセンス管理ファイル
エントリ番号 0
1532
コンテンツファイル
{Dc}
Data-inf
1522
ライセンス管理ファイル
エントリ番号 1
1533
コンテンツファイル
{Dc}
Data-inf
1523
ライセンス管理ファイル
ライセンス無
153n
コンテンツファイル(AA)
{Dc}
Data-inf
152n
ライセンス管理ファイル
エントリ番号 m
ライセンス管理デバイス520
ライセンス領域5215B
トランザクションID
コンテンツID
Kc
ACm
ACp
0
1
2
m
N-1
CD-ROM
コンテンツリストファイル
サーバ情報ファイル
801
コンテンツファイル
{Dc}
Data-inf
602
コンテンツファイル
{Dc}
Data-inf
603
コンテンツファイル(AA)
{Dc}
Data-inf
60n
コンテンツファイル
{Dc}
Data-inf

【図２２】


121
120
70
71
パーソナル
コンピュータ
50
モデム
40
60
30
10
配信サーバ

【図２０】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I		テーマコード（参考）
G10K 15/02		H04L 9/00		675B
G10L 11/00		G10L 9/00		E
H04L 9/08		H04L 9/00		601C
				601E

(71) 出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71) 出願人　000004167
日本コロムビア株式会社
東京都港区赤坂４丁目14番14号
(72) 発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72) 発明者　上村　透
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72) 発明者　畠山　卓久
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72) 発明者　高橋　政孝
石川県河北郡宇ノ気町字宇野気ヌ98番地の２　株式会社ピーエフユー内
(72) 発明者　常広　隆司
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所システム開発研究所横浜ラボラトリ内

(72)発明者　大森　良夫
神奈川県川崎市川崎区港町５番１号　日本コロムビア株式会社川崎工場内

Ｆターム(参考)　5J104 AA07 AA13 AA15 AA16 EA06
EA19 KA02 KA05 NA02 NA03
NA06 NA35 NA37 NA38 NA41
NA42 PA07 PA11